ARISTIDES TORAO FUTATA
OSNI VITO

DOCUMENTO ELETRÔNICO COMO MEIO PARA SUBSIDIAR PROVA NA CONSTATAÇÃO DO ILÍCITO TRIBUTÁRIO

Monografia apresentada ao Departamento de Contabilidade, do Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná, como requisito para obtenção do título de Especialista em Auditoria Integral.

Orientador: Prof. Blênio César Severo Peixe

CASCAVEL
2003

AGRADECIMENTOS

Agradecemos primeiramente a Deus, que é Pai e que nunca abandona seus filhos. Nossa conquista de hoje é mais uma expressão dessa certeza.

Agradecemos por nos ter dados forças e coragem para vencer todos os obstáculos que apareceram não permitindo que o desânimo e o cansaço nos abatessem nessa trajetória, muitas vezes dura e repleta de desafios.

Que a força e sua luz continuem a nos iluminar !

Agradecemos às nossas famílias – esposas e filhos – pela compreensão e incentivo ajudando-nos a preservarmos o propósito do aperfeiçoamento de nossa formação profissional e pessoal. Essa força fez e faz a diferença em nossas vidas. Obrigado!

Aos colegas de curso com quem assumimos o desafio como uma luta conjunta. Que os laços de amizade que se formaram, fortaleçam e sejam eternizados. Nossos agradecimentos e nossa amizade!

Aos mestres por compartilharem conosco seus conhecimentos e experiências profissionais, dedicando-nos precioso tempo de suas vidas.

Expressamos neste momento nossos agradecimentos e respeito!

À nossa Coordenação da Receita do Estado, que disponibilizou e incentivou-nos a realizar esse curso de especialização, dando-nos condições e meios para torná-lo possível.

A todos aqueles que , direta ou indiretamente colaboraram para que mais este objetivo fosse alcançado. Nosso muito obrigado !

DEDICATÓRIA

Às nossas famílias – esposas e filhos – pelo apoio e compreensão , em especial quando das nossas constantes ausências do lar para que a meta hoje alcançada pudesse ser possível. Vocês que estiveram presentes nos momentos mais difíceis dessa caminhada, que representam parte de nossas aspirações, fontes de nossos sucessos, razões de nosso viver, partilham conosco desta luta, abdicando de nosso tempo e atenção em favor do ideal que almejávamos. Nossa vitória é de vocês também. A vocês nosso carinho e gratidão. Deus lhes abençoe sempre.

RESUMO

FUTATA, A.T., VITO, O. **DOCUMENTO ELETRÔNICO COMO MEIO PARA SUBSIDIAR PROVA NA CONSTATAÇÃO DO ILÍCITO TRIBUTÁRIO.** Esse trabalho teve como objetivo subsidiar futuras auditorias. Mais especificamente buscou-se identificar os principais aspectos relacionados ao documento eletrônico; demonstrar os aspectos técnicos, práticos e legais da assinatura digital; analisar a prova documental como conceito jurídico. Para tanto, a matéria foi abordada com enfoque no seu conceito, nos mecanismos que garantem sua autenticidade e a identificação de sua autoria, sua diferenciação e equiparação do documento tradicional e ao final seus aspectos legais frente a legislação brasileira. Desta forma, propôs-se a elucidar o que é o documento eletrônico, sua utilidade e seu real funcionamento bem como seu processo de regulamentação. Concluiu-se que a falta de regulamentação e atribuição de validade jurídica aos documentos digitais representa, hoje, um dos maiores entraves do comércio eletrônico, pois a sociedade não confia plenamente nos documentos digitais exigindo como prova do negócio firmado através dos arquivos eletrônicos outros elementos de prova que o confirmem. A fim de garantir o reconhecimento da autoria e da integridade do conteúdo das declarações no documento digital, utiliza-se a nova tecnologia denominada assinatura digital. Assim, as assinaturas digitais podem ser consideradas como meio direto de prova dos contratos entre ausentes, celebrados por documento digital, todavia, o Brasil deve adotar uma legislação que garanta a validade dos documentos digitais garantindo segurança à sociedade global de que os negócios foram realmente concretizados, visto que não haverá como uma das partes se esquivar das obrigações por ela assumidas, alegando que este não foi efetivado, em razão do instrumento utilizado. Pode-se considerar que a validade jurídica dos documentos digitais dependerá da prévia garantia de sua segurança, pois primeiramente a lei deverá atribuir a tais documentos mecanismos que garantam a segurança da autoria, da autenticidade e tempestividade, para, assim, dar-lhes validade jurídica como prova documental.

Palavras chave: Documento Eletrônico, Prova Documental, Assinatura Digital, ICMS, Ilícito Tributário.

E-mail: aristides t futata@pr.gov.br

osnivito@pr.gov.br

ÍNDICE

1. INTRODUÇÃO

O progresso da ciência sempre traz consigo uma mudança nos hábitos e comportamentos das pessoas. E destes novos relacionamentos humanos surgem novas relações jurídicas, ou novos fatos jurídicos a serem objeto de regulação por parte do Direito. Nunca, porém, o avanço da tecnologia se fez tão presente no cotidiano como ocorre nos dias de hoje, com a informática. De acordo com MARCACINI (2003, p.1), "o fenômeno se destaca não só pela multiplicidade de usos que se pode dar a um computador, mas também pela popularização que esta tecnologia alcançou alterando sensivelmente o modo de vida da sociedade".

Esta popularização do uso da informática, seguida pela expansão da *internet,* colocou em evidência a expressão "documento eletrônico", termo que passou a integrar o vocabulário comum das pessoas, enquanto usuários do computador.

As transações eletrônicas, atualmente, são governadas por uma complexa e inconsistente mistura de diferentes aspectos, envolvendo jurisprudências, a aplicação da analogia (quando cabível) e várias instruções normativas, muitas destas relacionadas a assuntos diversos do comércio eletrônico. O desencontro dessas normas legais contribuem para a incerteza que circunda esse tipo de transação.

O uso cada vez mais amplo de computadores na vida social e, em particular, a difusão de transferências eletrônicas de fundos, a explosão da *internet* e o comércio eletrônico, leva à incontestável conclusão de que cedo ou tarde a sociedade terá de se valer de algum tipo de documento proveniente de um sistema de elaboração eletrônica, seja ele recibo de pagamento emitido por um terminal eletrônico de um banco, um ingresso para o cinema ou teatro comprado *on-line*, a inscrição para um concurso público cuja taxa foi debitada automaticamente em seu cartão de crédito, entre outros.

Sabe-se que na prática diária dos juristas o documento eletrônico já representa um avanço. Segundo GICO JÚNIOR (2003, p.1), "a maioria dos Tribunais já disponibilizou sua jurisprudência e acompanhamento processual pela *internet.*" E

a cópia impressa de julgados, ainda que sem autenticação é aceita pelos próprios Tribunais para caracterizar divergência de julgados, desde que indicada a fonte.

Um fenômeno social de tal magnitude impõe análise aprofundada. Urge em outros termos, indagar-se: Qual a validade jurídica dos documentos eletrônicos? Parte-se do pressuposto de que a sociedade moderna estruturou-se de forma indissociável sobre a tecnologia dos computadores e dos aparelhos eletrônicos. Assim sendo, não é difícil prever que, em breve período de tempo, toda a atividade de armazenamento de documentação se desenvolverá, salvo casos excepcionais, de forma digitalizada. Consequentemente, o documento dito cartular, isto é, o documento redigido pelas formas tradicionais, perderá grande parte de seu uso e importância social em favor do documento eletrônico.

Assim sendo, essa pesquisa, justifica-se à medida que pretende demonstrar o valor probatório dos documentos eletrônicos. Para tanto, busca-se abordar a matéria com enfoque no seu conceito, nos mecanismos que garantem sua autenticidade e a identificação de sua autoria, sua diferenciação e equiparação do documento tradicional e ao final seus aspectos legais frente a legislação brasileira. Desta forma, propõe-se a elucidar o que é o documento eletrônico, sua utilidade e seu real funcionamento bem como seu processo de regulamentação.

Neste sentido, espera-se contribuir com todos aqueles que direta ou indiretamente estejam envolvidos em situações fiscais que exigem uma maior compreensão do problema suscitado.

Esse trabalho, portanto, tem como objetivo subsidiar futuras auditorias. Mais especificamente busca-se:

- Identificar os principais aspectos relacionados ao documento eletrônico;
- Demonstrar os aspectos técnicos, práticos e legais da assinatura digital;
- Analisar a prova documental como conceito jurídico.

2. METODOLOGIA

Os objetivos específicos foram abordados pela técnica de pesquisa bibliográfica, segundo os indicadores da área Jurídica.

- Identificação dos principais aspectos relacionados ao documento eletrônico;
Contexto histórico: a sociedade da informação
Tratamento e armazenamento das informações
Informática (Computadores) e a telemática (rede *internet)*
Comércio Eletrônico
Documento eletrônico

- Demonstração dos aspectos técnicos, práticos e legais da Assinatura Digital.
Conceituação.
Regulamentação da assinatura digital no Brasil.

- Análise da prova documental como conceito jurídico.
Documento eletrônico como documento probatório.
A falsidade documental.
A negativa da autoria: a questão do ônus da prova.
Ilícito tributário e o comércio eletrônico.
Regulamentação do comércio eletrônico.

3. DESENVOLVIMENTO DO TRABALHO

Nesta parte do trabalho, pretende-se explicitar os aspectos relevantes do atual contexto com enfoque no contexto histórico da sociedade da informação, tratamento e armazenamento das informações, informática (computadores) e a telemática (rede *internet*), o comércio eletrônico, documento eletrônico. Posteriormente, versa sobre as técnicas de criptografia ressaltando a criptografia simétrica e assimétrica. Ressalta-se os documentos eletrônicos baseados no modelo "Firma Digital/Autoridade Certificadora" com ênfase na aposição de uma firma digital sobre um documento eletrônico. Por fim, aborda o documento eletrônico como meio de prova.

3.1. ASPECTOS RELEVANTES DO ATUAL CONTEXTO

Os itens abaixo apresentam a análise do contexto histórico da sociedade da informação, o tratamento e armazenamento das informações, a informática e a telemática, o comércio eletrônico e o documento eletrônico.

3.1.1. Contexto Histórico: a Sociedade da Informação

O mundo passa por transformações cada vez mais rápidas, seja no campo tecnológico, seja nos campos econômico e social. Um indivíduo nascido no século XIX ou anteriores, poderia passar toda a sua vida diante de uma realidade praticamente imutável, na qual o seu conhecimento e as coisas com as quais tal conhecimento se relacionava mantinham-se numa situação de relativa estabilidade. Um cidadão, transposto no tempo, do início do século XIX para o seu final, praticamente não sentiria nenhum choque cultural, pois suas habilidades lhe permitiriam permanecer apto a levar uma vida normal.

A partir do século XX, contudo, principalmente da década de 50 até os dias atuais, as mudanças em todas as áreas começaram a suceder-se de uma forma vertiginosa. A cada década o mundo e a sociedade confrontam-se com significativas alterações. Um cidadão do início do século XX, se transportado para os nossos dias, tornar-se-ia um ser anacrônico, deslocado culturalmente e desprovido das mais básicas habilidades necessárias à vida normal desse caótico mundo às portas do terceiro milênio.

Em fins do século XIX, tinha-se os primeiros passos da Revolução Industrial, o início da afirmação daquilo que viria a chamar-se a Sociedade Industrial. Em fins do século XX, vive-se o limiar da Revolução da Informação, destinada a levar os seres humanos a uma nova era, que vem sendo chamada de Sociedade da Informação. A preparação das nações para o ingresso nessa nova era é um fato. Estudos estão sendo desenvolvidos no mundo todo, visando compreender o fenômeno e, assim, instrumentar os países para que possam fazer a transição necessária de maneira segura e organizada.

> [...] um exemplo de tal abrangência e seriedade com que as iniciativas estão sendo tomadas, ao menos nos chamados países desenvolvidos, pode ser encontrado no chamado "Bangemann Report", elaborado no ano de 1994, por um grupo e estudos de alto nível a pedido do *European Council*. Ali estão definidos uma série de procedimentos e meios necessários para implementação de um amplo programa operacional voltado para as exigências da Sociedade da Informação (BANGERMANN, 1994, p. 06).

A expressão 'Sociedade da Informação' refere-se a um modo de desenvolvimento social e econômico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas, desempenham um papel central na atividade econômica, na criação de riqueza, na definição da qualidade de vida dos cidadãos e das suas práticas culturais.

A sociedade da informação corresponde, por conseguinte, a uma sociedade cujo funcionamento recorre crescentemente a redes digitais de informação. Esta alteração do domínio da atividade econômica e dos fatores determinantes do bem-estar social é resultante do desenvolvimento das novas tecnologias da informação, do audiovisual e das comunicações, com as suas importantes ramificações e

impactos no trabalho, na educação, na ciência, na saúde, no lazer, nos transportes e no ambiente, entre outras.

De acordo com AUGUSTO (1993, p. 46), "as tecnologias da informação e das comunicações são já parte integrante do nosso quotidiano. Invadiram as nossas casas, locais de trabalho e de lazer". Para esse autor, oferecem instrumentos úteis para as comunicações pessoais e de trabalho, para o processamento de textos e de informação sistematizada, para acesso a bases de dados e à informação distribuída nas redes eletrônicas digitais, para além de se encontrarem integradas em numerosos equipamentos do dia a dia, em casa, no escritório, na fábrica, nos transportes, na educação e na saúde. A sociedade da informação não pertence a um futuro distante. Assume uma importância crescente na vida coletiva atual e introduz uma nova dimensão no modelo das sociedades modernas.

Portanto, fica claro que, na Sociedade da Informação, o poder se centralizará no domínio da informação, aí compreendidos não só o acesso a ela, mas também o seu tratamento, a capacidade de tornar dados brutos e desprovidos de sentido em informações lapidadas e plenas de significado. Sendo as diversas formas citadas de abordagem da informação – a aquisição, o armazenamento, o processamento, a valorização, a transmissão e a disseminação de informação – questões de crucial relevância no panorama desenhado, nada mais lógico do que abordar matérias significativas dentro de tais temas, em subtópicos específicos, conforme far-se-á a seguir.

3.1.2. Tratamento e Armazenamento das Informações

Pode-se iniciar o assunto com a afirmativa: obter-se dados é relativamente fácil, ao passo que obter-se uma informação é algo relativamente trabalhoso. Isso porque a informação é o resultado do tratamento dos dados. O exemplo prático a seguir pode ajudar a entender melhor essa distinção inicial.

O IRS (*Internal Revenue Service*), a Receita Federal dos Estados Unidos, coleta, administra e contabiliza mais de 200 milhões de formulários por ano, o que resulta em mais de 1,4 bilhão de folhas de papel4. Esses milhões de formulários contêm dados brutos e em quantidade tão grande que, em tal estado, representam o

mesmo que nada em termos de conhecimento. Somente após receberem o devido tratamento, à custa de muitas horas de trabalho de muitas pessoas, é que se pode extrair dos dados condensados algumas informações úteis (dentre as quais, possivelmente, a que mais deve interessar ao IRS seja "quem deve" e "quanto é devido", em relação aos tributos ali administrados).

Em termos técnicos, a distinção entre dado e informação apresenta certa importância. No âmbito do presente trabalho, contudo, tal diferenciação não possui maior relevância, sendo ambos os termos tratados como equivalentes, normalmente utilizando-se o termo "informação" com significado genérico, e mencionando-se o termo específico "dado" somente onde se fizer necessária uma maior precisão.

> Assim como dados geram informações, estas, tratadas, também podem gerar novas informações, num processo de auto-alimentação. Quanto mais desenvolvida é a sociedade, mais dados e informações ela detém. Um exemplo pitoresco que se costuma citar a respeito do volume de papel envolvido nas atividades modernas, dá conta que, se um avião Boeing 747 fosse carregado com todos os documentos relativos ao seu projeto, fabricação, operação, manutenção e outros, ele não conseguiria decolar (AUGUSTO, 1993, p. 35).

Obviamente, as pessoas não guardam todo esse conhecimento em suas próprias cabeças. Ainda nos dias de hoje, o maior suporte de armazenamento permanente de dados e informações é o conhecido papel. Apesar do surgimento da informática e dos novos meios de tratamento de dados, tal supremacia do papel ainda não está ameaçada. Segundo BRASIL (2002, p. 05) "A razão maior está num aparente paradoxo: quanto mais intensamente se tem utilizado a informática, mais fácil torna-se o tratamento dos dados, mais informações são criadas e mais papel é gerado"

As informações armazenadas em computadores ainda são poucas em relação ao total, mas a tendência irreversível é que o papel perca espaço cada vez mais rapidamente. Conforme MERCADO (2002, p. 94) "E não apenas em razão das dificuldades de manuseio e tratamento das informações que o meio tradicional apresenta, mas sim em razão, principalmente, do enorme custo que tais atividades acarretam" BUONOMO (2003, p. 09) cita em artigo no qual aborda os atos e documentos eletrônicos, que um estudo da Autoridade para Informática na Administração Pública (órgão governamental italiano), feito em 1994, "apurou que a despesa pública anual, somente com atividades de registro e arquivamento de

documentos em papel, chega a 150 bilhões de liras (o equivalente a cerca de 90 milhões de dólares)". Ao mesmo tempo, considerando-se a despesa global – compreendendo-se, aqui, as horas de trabalho gastas na pesquisa e compilação de formulários, mais a perda de horas trabalhadas em razão da pesquisa ou apresentação de documentos requeridos à Administração Pública – varia dos 10 aos 15 trilhões de liras ao ano (o equivalente a algo entre 600 e 900 milhões de dólares).

> A disciplina do documento informático e da firma digital se enquadra, portanto, no contexto geral de reforma da administração pública e da renovada relação entre a administração pública e os cidadãos em uma ótica de maior eficiência e racionalidade das ações administrativas e de contenção da despesa pública (BUONOMO, 2003, p. 09).

Observa-se, portanto, que armazenar e tratar informações são tarefas de grande relevância dentro do mundo e da sociedade contemporâneos. Conjuntamente com essa constatação, observa-se que todos os caminhos conduzem ao uso intensivo da informática e da telemática como ferramentas aptas para um desempenho mais racional, menos dispendioso e mais eficiente na execução das citadas tarefas. Por essa razão, tais ferramentas serão abordadas no próximo subtópico.

3.1.3. Informática (Computadores) e a Telemática (Rede Internet)

Inicialmente, quando de seu surgimento na década de 40, os computadores foram tidos como enormes máquinas de calcular, operadas misteriosamente por uma categoria de cientistas um tanto suspeitos, dotados sabe-se lá de que estranhos poderes capazes de permitir a eles entenderem aquele exótico emaranhado de válvulas e fios. Eram máquinas tão sem propósito que muitos duvidavam que um dia viriam a ter alguma serventia, em função de seu gigantesco tamanho e da sua impensável complexidade de manejo. A aplicação de um computador em alguma atividade cotidiana era, então, inimaginável.

As constantes inovações tecnológicas havidas nos últimos anos propiciaram o surgimento de uma imensa gama de novas aplicações para os computadores e para a informática. A partir da década de 80 e, mais notadamente, da década de 90, é tal

a sua utilização no cotidiano de todas as pessoas – seja em suas atividades pessoais seja em seus negócios, no mundo todo –, que não é fantasia afirmar-se que uma crescente dependência vai tomando corpo. O espaço antigamente ocupado pelas comuníssimas máquinas de escrever, citando-se apenas um exemplo dessa popularidade, foi quase que completamente tomado pelos computadores.

Pode-se usar o computador para as mais diversas atividades, desde as mais básicas e já costumeiras como a digitação e edição de textos, arquivamento e manutenção de bancos de dados, elaboração de relatórios, processamento de dados diversos, até as mais recentes, chamadas aplicações multimídia, que proporcionam o tratamento e manipulação de sons, fotografias e imagens de vídeo. De acordo com MERCADO (2002, p. 67) "com grande chance de acerto, que são poucas as atividades modernas que não se beneficiariam fazendo algum uso do computador".

Até aqui, tratou-se do computador em si considerado, como uma unidade isolada, aplicado em tarefas que operavam com informações armazenadas localmente, na própria máquina. Acontece que, conjuntamente com a grande evolução da informática, deu-se uma grande evolução das telecomunicações. Da junção da informática com as telecomunicações surgiu a telemática. A partir daí, um computador passou a poder comunicar-se com outros computadores, trocando informações, possibilitando, com isso a circulação instantânea e sem limites das informações que, antes, eram estáticas e permaneciam circunscritas ao alcance físico das pessoas. Surgiram, assim, as chamadas "redes de computadores", que nada mais são do que grupos de computadores interligados mediante o uso de alguma forma de telecomunicação.

Com as redes, surgiu o chamado EDI (*Electronic Data Interchange*), que trata da transferência, computador a computador, de mensagens estruturadas segundo determinado padrão e atendendo a determinada convenção estipulada entre os participantes. Com o EDI, através da ligação dos bancos de dados de dois ou mais sujeitos, sem a necessidade de intervenção humana para a execução das operações de transmissão, informações as mais diversas são intercambiadas, atendendo-se aos mais diversos fins (por exemplo, remessas periódicas de

informações de controle de uma organização para outra ou, mais, recentemente, transações comerciais).

O uso das redes foi-se popularizando de tal forma que, hoje, um computador que não esteja "em rede" tornou-se uma máquina de possibilidades muito limitadas. Criaram-se grandes redes corporativas (de organizações específicas) e criou-se, especialmente, a maior rede de todas, a Internet, que é uma rede onipresente, acessível nos mais distantes rincões do planeta, onde haja uma simples linha telefônica disponível (aliás, atualmente, com as comunicações via satélite ou com a possibilidade de acesso via cabo e ondas de rádio, nem isso é mais tão necessário). Interligado pela Internet, o mundo nunca esteve tão perto de se tornar, de fato, a "aldeia global" de que falava Marshall McLuhan, conhecido teórico canadense da comunicação de massa. O outro lado do mundo passou a estar tão ou mais acessível do que o nosso próprio vizinho. Nessa linha de raciocínio, MICCOLI situa a Internet da seguinte forma:

> Realmente o mercado está numa avançada via de transformação, a qual os sociólogos mais atentos há tempos chamam de *aldeia global*; esta aldeia global que compreende o planeta inteiro já tem a sua praça, a rede informática *Internet*. Esta praça já possui numerosos locais de encontro, os *web sites*, os abrigos de seus freqüentadores, os grupos de discussão e, sobretudo, um número de visitantes já calculável em dezenas de milhões (MICCOLI, 2003, p. 1).

Compreendida de forma genérica, a Internet se apresenta como um mecanismo de formação de uma verdadeira comunidade mundial, que não reconhece as fronteiras geopolíticas tradicionais. Trata-se de uma rede de extensão planetária, de contornos indefinidos e cujo acesso é de baixo custo. As tentativas de regulação do fenômeno são incipientes, as restrições legais são poucas e ainda não existem entidades reguladoras realmente eficazes. A Internet, portanto, é um novo espaço, começando a ser desbravado.

Pelos caminhos da Internet circulam, diariamente, informações diversas e com as mais variadas características. Nela convivem o trabalho, o estudo e o lazer. Operações bancárias e comerciais são efetuadas, cartas pessoais ou de negócios são enviadas de um extremo a outro do planeta, mensagens de toda espécie são trocadas e, mesmo, inúmeros contratos são celebrados mediante tão fascinante e cômoda forma eletrônica.

Configura-se, assim, como resultado da junção da informática com as telecomunicações (telemática), em meio a toda uma atividade frenética, um novo centro de fenômenos jurídicos dotados de invulgar complexidade e de crescente inadequação aos ordenamentos vigentes. Conforme ALEXANDRE (2003, p. 3) "é o chamado "ciberespaço", formado pelas redes de computadores, uma dimensão onde tudo acontece virtual e simultaneamente". Para esse autor, ali misturam-se acontecimentos e aspectos de relevância jurídica os mais diversos, como o comércio, a liberdade de expressão, o domicílio, o dano, o contrato, o pagamento, a privacidade, os direitos autorais e incontáveis outros.

Segundo LIMA NETO (2003, p. 9) "a Internet propiciou o surgimento de uma nova sociedade, uma sociedade ao mesmo tempo virtual e global". O autor considera que essa sociedade, formada de estratos culturais heterogêneos, tornou possível o aparecimento do denominado 'mundo virtual' ou 'ciberespaço.

Pode-se dizer que essa é a nova realidade (ou seria virtualidade?) proporcionada pelas inovações tecnológicas descritas, afetas aos campos da informática e da telemática. Toda a facilidade de comunicação e de relacionamento instantâneo entre pessoas e países, propiciada pelos novos meios, resultou em uma sensação de redução de distâncias, do planeta Terra, acabando por desencadear um processo de compreensão do mundo como uma unidade não definida a partir das meras fronteiras entre países. A tal processo denominou-se "globalização" e, na sua esteira, vieram novos conceitos políticos, econômicos e sociais. Em termos econômicos, houve a criação de uma imensa massa de capitais errantes e uma grande intensificação do comércio internacional.

> Com o advento da revolução digital e da concorrência à escala global, muitas empresas começaram a explorar as novas oportunidades de mercado, desenvolvendo áreas de negócio até então inexistentes. O crescimento do mercado das comunicações móveis, a explosão da Internet, a emergência do comércio eletrônico, o desenvolvimento da indústria de conteúdos em ambiente multimídia, a confluência dos setores das telecomunicações, dos computadores e do audiovisual, demonstram o enorme potencial das tecnologias de informação para gerar novas oportunidades de emprego, estimular o investimento e o desenvolvimento acelerado de novos setores da economia (AUGUSTO 1993, p. 35).

Para o autor acima citado o comércio sempre esteve na vanguarda das novas tendências e movimentos mundiais (basta citar o exemplo dos chamados grandes descobrimentos e navegações de espanhóis e portugueses). Nos tempos atuais,

mais do que nunca, comerciar é preciso. O novo mundo globalizado passou a ser olhado como um mercado consumidor com enormes nichos a serem conquistados. A vantagem é que, hodiernamente, não é apenas lançando-se caravelas e galeões ao mar que se pode comerciar. As transações comerciais podem ser efetuadas à distância, sem que nenhuma das partes necessite sequer sair do conforto de suas poltronas: trata-se do comércio eletrônico, tema objeto do subtópico seguinte.

3.1.4. Comércio Eletrônico

O incremento do comércio eletrônico nos últimos anos, bem como a grande prioridade que muitos países têm dado ao seu desenvolvimento se deve às enormes vantagens que ele pode oferecer.

O comércio eletrônico permite fazer negócios por via eletrônica. Baseia-se no processamento e transmissão eletrônica de dados, incluindo texto, sons e imagem.

Abrange atividades muito diversas, que incluem o comércio eletrônico de bens e serviços, a entrega em linha de conteúdo digital, as transferências financeiras eletrônicas, o comércio eletrônico de ações, conhecimentos de embarques eletrônicos, leilões comerciais, concepção e engenharia em cooperação, determinação em linha das melhores fontes para aquisições, contratos públicos, comercialização direta ao consumidor e serviços após venda. Envolve quer produtos (por exemplo, bens de consumo, equipamentos médicos especializados) quer serviços (por exemplo, serviços de informação, serviços financeiros e jurídicos), atividades tradicionais (por exemplo, cuidados de saúde, educação) e atividades novas (por exemplo, centros comerciais virtuais).

É freqüente hoje em dia as empresas transferirem através da Internet, funções, como a execução de encomendas e envios, para distribuidores especializados nesses serviços. De acordo com AUGUSTO (1993, p. 69), "os próprios distribuidores estão a tornar-se 'virtuais', transferindo a armazenagem e o movimento de mercadorias físicas para especialistas em logística, como empresas privadas de correio expresso". As livrarias e lojas de discos da Internet com maior êxito na Europa e nos Estados Unidos são assim verdadeiras 'empresas virtuais': as encomendas e o transporte são feitos diretamente dos armazéns das editoras e as

bases de dados dos fornecedores estão plenamente integradas com as empresas de transporte.

Do exposto, pode-se inferir que a redução de custos obtida com tal sistemática é brutal. A racionalização das operações é uma das maiores possibilidades do comércio eletrônico. A movimentação física de mercadorias diretamente de sua origem para o seu destino final, sem passagem por locais intermediários, por si só, já torna a prática extremamente atrativa para os comerciantes em geral (mais ainda para os próprios fabricantes). Isso sem contar com a exposição mundial que as empresas podem usufruir, institucionalmente ou relativamente a algum de seus produtos específicos, uma vez implementada uma disponibilização via acesso pela Internet. Sob esse aspecto, trata-se, mesmo, de uma democratização da concorrência, pois até as pequenas empresas terão um canal de acesso ao mercado em condições de relativa igualdade com as empresas maiores. Isso porque a abertura de uma "loja virtual" na Internet não requer tantos gastos quanto a abertura de um estabelecimento comercial no mundo físico real.

Contudo, apesar do comércio eletrônico já estar em operação em todo o mundo, ele ainda não conta com uma base sólida (ao menos, em termos jurídicos). MONTI (2003, p. 7) abordando as compras via Internet, permite entrever o problema: "Aparentemente se trata de uma coisa banal, se preenche um formulário com os próprios dados e com aqueles do cartão de crédito, um *clic* e tudo está feito. Tudo é baseado na confiança". O cliente envia os próprios dados no pressuposto de que os vendedores os utilizarão de modo correto, enviando-lhe exatamente o produto requerido e, de outra parte, o segundo confia no fato de que o número fornecido corresponda a um cartão de crédito regularmente portado. Quando tudo vai bem, não é possível ou necessário imaginar-se um sistema mais prático para comprar ou vender na rede, mas o que acontece em caso de controvérsia, sobretudo considerando que a compra acontece freqüentemente no escuro? Como se faz, por exemplo, para demonstrar que a ordem provinda via rede é efetivamente aquela enviada pelo cliente, no que se refere ao preço, qualidade e quantidade?

Observa MICCOLI (2003, p. 4), que o uso cotidiano dos cartões de crédito em compras telefônicas ou via Internet, nas quais não há nenhum documento assinado, "baseia-se na assunção do risco de mau funcionamento do sistema por parte de

quem oferece o serviço". O autor entende que isso é possível porque o volume das transações é muito grande, mas o valor de cada uma é relativamente baixo, resultando insignificantes, em relação ao todo, os eventuais problemas verificados. Segundo o autor, o comércio eletrônico vem se mantendo com base no mesmo princípio que tradicionalmente rege os contratos de seguro.

> À medida que cada vez mais transações comerciais são feitas por computador, que passam também a servir como meios de guarda de documentos, a Justiça terá que desenvolver métodos de aferição, para o caso de os dados serem envolvidos em algum litígio. 'Isso é uma questão que os juristas enfrentarão pelos próximos dez anos', avalia Thioller [Alexandre Thioller, advogado]. Ele mesmo tem como cliente uma empresa de redes locais, que opera todos os pedidos e emissões por correio eletrônico. Até hoje nunca houve contestação, mas ele admite que se alguém conseguisse entrar na rede com objetivos escusos, haveria dificuldades técnicas para se provar a fraude (AUGUSTO, 1993, p. 46).

Na opinião do autor citado acima, por um lado existem as questões técnicas destinadas a garantir um grau de segurança desejável. De outro lado, estão as questões jurídicas a serem examinadas e devidamente disciplinadas. Pode-se dizer, ainda, que ambas as matérias, a técnica e a jurídica, em muitos pontos se entrelaçarão. As implementações técnicas efetuadas somente poderão ser consideradas plenamente satisfatórias uma vez que, além de considerarem a excelência das soluções sob um ponto-de-vista eminentemente tecnológico, sejam capazes de atender, também, às exigências específicas determinadas pela ordem jurídica que venha a ser estabelecida.

A este respeito SAKAMOTO (2003, p. 11) afirma que "a informática poderá vir a tornar-se elemento catalítico de uma completa reestruturação dos pressupostos básicos de todo o sistema legal mundial, abrindo a oportunidade de integração dos sistemas nacionais em um sistema internacional e coerente". Fica evidente que a disciplina de uma atividade de caráter tão globalizado quanto pretende ser o comércio eletrônico, deve merecer um tratamento jurídico adequado, que não desconsidere tal condição. Ao mesmo tempo, como decorrência da própria globalização e formação de blocos regionais, o ordenamento interno de cada país, em muitos pontos, tenderá a buscar a uniformidade, o equilíbrio, com os demais ordenamentos envolvidos nessas novas relações.

Aponta-se em decorrência da nova realidade mundial, uma era de novidades também para o Direito. De um lado, pela citada necessidade de uniformização entre

os diversos ordenamentos jurídicos. De outro lado, pela necessidade de contato do Direito com as novas tecnologias que já não podem mais passar desapercebidas, impondo ao legislador a tarefa de editar normas capazes de regular complexas situações que em tal contexto vão, cada vez mais rapidamente, se apresentando e se consolidando. Uma dessas situações encontra-se, justamente, na existência de documentos eletrônicos juridicamente válidos. É sobre isso que trata o último subtópico desse breve contexto histórico que se pretendeu traçar.

3.1.5. Documento Eletrônico

Normalmente, quando se fala em "documento", logo se imagina uma página impressa em papel onde se encontra algum escrito que identifica uma pessoa ou registra um fato. No meio jurídico, pode representar um escrito que faz fé daquilo que atesta, de forma que, se apresentado em juízo, prova o que o litigante alega. No campo das obrigações, a idéia de documento sempre esteve ligada à imagem de algo escrito, com a perfeita identificação da pessoa, ou, no caso de um contrato, dos contratantes. Com o advento da Internet, o conceito de documento teve que passar por uma adequação, de forma a se tornar viável a sua aplicação no meio virtual, tendendo a alcançar os mesmos objetivos já consolidados no meio tradicional. Segundo MARCACINI (2003, p. 3) "partindo do conceito tradicional de documento, podemos verificar certa dificuldade inicial em nele abranger o documento eletrônico". CHIOVENDA, citado pelo autor acima, assim o definiu: "O documento, em sentido amplo, é toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente".

Entretanto, é interessante mencionar que, para alguns doutrinadores, o documento foi definido como sendo *"o escrito"*, e não como *"a coisa"*. Gabriel Rezende Filho citado por MARCACINI (2003, p. 10) ensinava que "instrumento público é o escrito lavrado por oficial público, segundo suas atribuições e com as formalidades legais", enquanto "instrumento particular é o escrito emanado do interessado ou interessados, sem a intervenção do oficial público". Ao definir o documento a partir do pensamento lançado em algum meio (que à época só poderia

ser algo tangível), ao invés de privilegiar *a coisa* onde o pensamento está lançado, estes últimos conceitos permanecem atuais.

> Podemos conceituar o documento eletrônico como sendo o que se encontra memorizado em forma digital, não perceptível para os seres humanos senão mediante intermediação de um computador. Nada mais é do que uma seqüência de *bits*, que por meio de um programa computacional, mostrar-nos-á um fato (GANDINI, et. al., 2003, p. 3).

Por sua vez, CASTRO assim define documento eletrônico:

> O documento eletrônico pode ser entendido como a representação de um fato concretizada por meio de um computador e armazenado em formato específico (organização singular de bits e bytes), capaz de ser traduzido ou aprendido pelos sentidos mediante o emprego de programa (*software*) apropriado (CASTRO, 2003, p. 1).

Um conceito atual de documento, para abranger também o documento eletrônico, deve privilegiar o pensamento ou fato que se quer perpetuar e não a coisa em que estes se materializam. Isto porque o documento eletrônico é totalmente dissociado do meio em que foi originalmente armazenado. Um texto, gravado inicialmente no disco rígido do computador do seu criador, não está preso a ele. Assumindo a forma de uma seqüência de *bits*, o documento eletrônico não é outra coisa que não a seqüência mesma, independentemente do meio onde foi gravado. Assim, o arquivo eletrônico em que está este texto poderá ser transferido para outros meios, sejam disquetes, CDs, ou discos rígidos de outros computadores, mas o documento eletrônico continuará sendo o mesmo.

Conforme BRASIL (2003, p. 6), historicamente os doutrinadores "têm definido o documento como algo material, uma *res*, uma representação exterior do fato que se quer provar e sempre conhecemos a prova documental como a maior das provas, pois consistente da representação fática do acontecido". Para esse autor, ao ligar indelevelmente o fato jurídico à matéria como uma coisa tangível, tem-se dificuldades em conceituar o documento eletrônico, pois este é intangível e etéreo, e muito longe se encontra do conceito de "coisa" como matéria.

Partindo-se do conceito conhecido de que o documento é uma coisa representativa de um fato, Moacyr Amaral Santos citado por MARCACINI (2003, p. 04) afirma que não se pode dizer que o documento eletrônico é um Documento, porque "ele não é uma coisa e, portanto, não pode ser representativa de um fato". O

autor entende que ao olhar pelo prisma do registro do fato, percebe-se que ele se adequa perfeitamente a este conceito, porque como uma seqüência de *bits* ele pode ser traduzido por meio de programas de informática que vão revelar o pensamento ou a vontade daquele que o formulou, exigindo do intérprete uma concepção abstrata para compreendê-lo.

Apesar de o documento eletrônico não se tratar de uma coisa palpável, visto que se encontra armazenado em outro meio que não o papel, isto não o inviabiliza de forma alguma como instrumento capaz de registrar um pensamento ou um fato, uma vez que pode ser acessado por programas específicos de computador que lêem seu conteúdo e o expõe através de meios de leitura apropriados para a leitura e compreensão humana (impressoras, vídeos, alto-falantes) tornando-se capaz de excitar os sentidos e transmitir ao homem qual é a idéia ou o fato que está registrando em si.

Para aqueles que insistem no fato de que o documento só é válido se for uma coisa palpável, pode-se dizer ainda que os documentos eletrônicos não se encontram em papel, mas sim em mídias magnéticas que têm a capacidade de armazenar dados digitais, isto é, feitos de *bits*, assim como o papel, uma mídia em celulose, tem a capacidade de armazenar dados impressos, isto é, feitos de tinta ou grafite.

Assim, ao se fazer o peticionamento eletrônico através de serviços de correio eletrônico ou *web,* o que está sendo protocolado é um documento tão inteligível quanto o documento tradicional. Para MARCACINI (2003, p. 11), "esta certeza é ainda maior se os documentos eletrônicos transmitidos não possuírem sons e/ou imagens animadas", ou seja, apenas mensagens escritas ou figuras estáticas, pois tudo aquilo que for transmitido (em formato digital) poderá ser convertido em documento físico, uma vez que poderá ser impresso em papel e fazer parte dos autos do processo ao qual se destinam.

É importante salientar que, embora os documentos eletrônicos que possuam sons e imagens animadas possam vir a ter a mesma validade dos documentos eletrônicos que possuam apenas texto ou imagens estáticas, aqueles não são aceitos para se fazer o peticionamento eletrônico, pois, conforme o art. 1º da Lei 9.800/99, é permitida às partes a utilização de sistema de transmissão de dados e

imagens tipo fac-símile ou outro similar, apenas para a prática de atos processuais que dependam de petição escrita, o que, portanto, não é o caso de sons e animações.

Porém, no caso dos documentos eletrônicos encontra-se uma dificuldade: como ter certeza de que o documento recebido pelo órgão judiciário através do peticionamento eletrônico realmente foi transmitido por determinada pessoa? E se tivermos a certeza de quem é seu remetente, como ter certeza de que o documento não foi alterado durante sua transmissão por pessoas mal intencionadas? Ou seja, como ter certeza de que o documento recebido pelo órgão judiciário possui autenticidade e/ou integridade? Para isso, a ciência da informática utilizou-se de uma antiga ciência: a criptografia, de que será tratado a seguir.

3.2. TÉCNICAS DE CRIPTOGRAFIA

Existem, basicamente, duas grandes técnicas de criptografia, denominadas de criptografia simétrica e criptografia assimétrica. A principal diferença entre elas reside na maneira como seus criadores conceberam a criação e utilização das chaves. Ambas serão abordadas a seguir.

A criptografia vem sendo utilizada primariamente em assuntos de Estado, e possui muitas técnicas consagradas, algumas delas de inegável eficácia. Não obstante, a maioria dessas regras utiliza rígidas estruturas hierárquicas governamentais, necessitando mesmo de tais estruturas. Para GICO JÚNIOR (2003, p. 23), "o emprego de processos criptográficos em redes públicas de comunicação com conexões não hierarquizadas apresenta graves problemas administrativos, tais como distribuição de chaves, crescimento da rede, autenticação dos usuários e outros".

3.2.1. Criptografia Simétrica

A criptografia de chave simétrica, também conhecida como de chave secreta, é a mais antiga e, por isso, também é chamada de criptografia tradicional. Segundo

VOLPI (2001, p. 7) "é a técnica que, normalmente, se utiliza de uma única chave, vinculada tanto ao processo de cifragem quanto ao processo de decifragem". Essa vinculação pode ser total, no caso de uso da mesma chave para a execução dos dois processos, ou pode ser uma vinculação parcial, caso em que, apesar de ser utilizada uma chave para cifragem e outra para decifragem, a segunda pode ser deduzida em função do conhecimento da primeira.

Dessa forma, na técnica de criptografia simétrica, ainda que, eventualmente, possam existir duas chaves, não existe independência entre elas (o que as une como se fossem, na prática, uma só). A chave de cifragem, em qualquer caso, deverá ser conhecida por todo aquele que quiser efetuar a respectiva decifragem (seja para uso direto, seja para dedução da chave derivada a ser utilizada).

A criptografia de chave simétrica, conforme VOLPI (2001, p. 7) "é utilizada desde os primórdios da humanidade, tendo sofrido evolução em sua complexidade ao longo do tempo". Na opinião deste autor, tal fato pode ser inferido através dos dois métodos de criptografia de chave simétrica citados anteriormente: o método da "Substituição de César" e o método DES. Em relação ao primeiro, viu-se que se tratava de algo extremamente rudimentar, oferecendo um limitado número de 25 chaves e podendo o seu algoritmo ser executado, manualmente, sem grande esforço por uma pessoa sem quaisquer habilidades especiais.

> Apesar De eficaz, este método de codificação tem a desvantagem de ser facilmente decifrado. Para uma melhor visualização das chances de decifração, pode-se tomar como parâmetro o alfabeto ocidental, composto por 26 letras. Dessa forma, o interceptor teria que testar; no máximo, vinte e seis chaves possíveis, encontrando entre uma delas a correta (VOLPI, 2001, p.8).

Em relação ao segundo método, atual e muito mais avançado, trata-se de um algoritmo de execução impraticável sem auxílio de um computador, que oferece a possibilidade de uso de mais de 72 quatriliões de chaves distintas (isso, considerando-se a chave de 56 *bits* comum do método DES, ressaltando-se que cada aumento de um único *bit* no tamanho da chave resulta na dobra do número de chaves diferentes disponíveis).

Sobre a forma de uso da criptografia simétrica, GIUSTOZZI elabora uma analogia:

> Todos os cifradores tradicionais, de fato, se comportam na prática como se comporta a fechadura da nossa porta, que abrimos e fechamos com o uso da mesma chave. No caso específico, a chave criptográfica usada para cifrar uma mensagem é a mesma que depois será aplicada para decifrá-la. Um cifrador deste tipo se chama *simétrico* (GIUSTOZZI, 2003, p. 2).

A finalidade precípua do método de criptografia de chave simétrica é obtenção do sigilo dos dados, incrementando-se, assim, a sua segurança. O objetivo básico é evitar que pessoas não autorizadas possam ter conhecimento do teor de quaisquer informações julgadas confidenciais.

O principal problema relacionado com o método de criptografia de chave simétrica, segundo GIUSTOZZI (2003, p. 2) reside, justamente, "no fato de que as partes que necessitem utilizá-la deverão ter acesso à mesma chave criptográfica". Há, pois, que existir um acordo entre elas, no que diz respeito à chave a ser utilizada por todas. Só assim é que haverá possibilidade de cifragem e decifragem apropriada de dados, com os interessados podendo fazê-los circular, entre si, de forma segura e sigilosa.

Tal fato, já de início, acarreta dois sérios problemas de segurança, diretamente decorrentes do gerenciamento de chaves (*key management*) que se mostra necessário. O primeiro deles, diz respeito à utilização e conservação do segredo de uma chave que é de conhecimento de várias pessoas. Bastaria uma delas agir de forma culposa ou, pior, de forma dolosa, para que todos sofressem as eventuais conseqüências. O segundo problema refere-se à própria distribuição da chave, em si. Sempre que uma nova pessoa fosse admitida no grupo, necessitaria receber essa chave, com boa segurança no respectivo processo de envio (note-se que, para isso, seria desejável que a chave enviada também estivesse criptografada, gerando-se, assim, uma espécie de círculo vicioso). Vê-se, pois, que o momento e a forma de trânsito da chave, são fatores de sério risco para a integridade da segurança proporcionada pela criptografia simétrica. Tais dificuldades de gerenciamento de chaves, sem dúvida, limitaram bastante a popularização de uso da criptografia simétrica.

Os problemas, na distribuição e manutenção do segredo das chaves simétricas, ficam minimizados quando a circulação de dados criptografados é feita sempre para um só destino, pelo fato das origens, ainda que diversas, transmitirem sempre os mesmos dados, já devidamente cifrados. Para GIUSTOZZI (2003, p. 2)

"esse é o típico caso, por exemplo, do uso de cartões eletrônicos bancários, que contêm dados já previamente cifrados (gravados na tarja magnética), os quais são transmitidos para o banco sempre que for utilizado o cartão". O autor comenta ainda que o destinatário, o banco, deverá decifrar os dados recebidos, uma vez que foi ele quem já os cifrou quando da emissão dos cartões.

Devido a essa característica de ser apenas ele (o banco) quem possui a tarefa de decifragem de dados, a chave criptográfica utilizada nunca precisa sair do seu controle e dos seus domínios. Os usuários de cartões, portanto, não têm a menor necessidade de possuir qualquer chave ou, mesmo, ter qualquer conhecimento sobre a existência da criptografia.

Atualmente, ainda é largamente utilizado o método de criptografia de chave simétrica (notadamente para transações bancárias eletrônicas, conforme exemplo), sendo que seus os algoritmos mais conhecidos são o já citado DES (*Digital Encryption Standard*), que usa uma chave com tamanho de 56 *bits* e o IDEA (*International Data Encryption Algorithm*), que usa uma chave com o tamanho de 128 *bits*.

3.2.2. Criptografia Assimétrica

No caso da criptografia de chave assimétrica, também chamada de criptografia de chave pública, não se utiliza apenas uma chave, mas sim um par delas. Uma chamada de chave pública (*public key*), destinada a ser do livre conhecimento de todos, e outra chamada de chave privada (*private key*), destinada a ser mantida secreta sob custódia exclusiva de seu proprietário. Esse par de chaves pode ser visto como relativamente independente entre si. Esse atributo de "independência relativa" pretende significar que não deve ser possível deduzir-se uma chave a partir do conhecimento da outra. Ele decorre de dois fatores básicos: da geração adequada do par de chaves e do particular uso matemático que delas faz o algoritmo assimétrico.

Observe-se que a independência é dita "relativa" porque ela somente será efetiva se forem geradas chaves com tamanho maior ou igual a um tamanho mínimo especificado, aceito pelos estudiosos da matéria como capaz de propiciar um nível

de segurança razoável (ou seja, tornar praticamente impossível a dedução de uma chave a partir do conhecimento da outra).

> Com o uso da criptografia assimétrica para gerar assinaturas eletrônicas, vê-se que é possível criar um vínculo entre a assinatura o corpo do documento, impedindo a sua alteração posterior. Entretanto, o direcionamento da proteção é o outro: o documento, em si, continua podendo ser alterado, sem deixar vestígios no meio físico, mas se isto for feito, ele perderá o vínculo que mantém com a assinatura, tornando-se apócrifo e, com isso, perdendo todo o seu valor probante (MARCACINI, 2003, p. 14).

A geração e o uso de chaves com tamanho inadequado (pequeno demais) comprometeria a verdade da afirmativa, pois isso poderia tornar possível – mediante uso de computadores poderosos para a aplicação das devidas fórmulas matemáticas –, a dedução de uma chave a partir do conhecimento da outra chave do par (note-se ser necessário, também, o conhecimento de alguns dados cifrados pela chave que se tenta deduzir). Sobre a relatividade da independência das chaves no sistema de criptografia assimétrica, BUONOMO corrobora a advertência feita:

> [...] o conhecimento da chave pública não deve fornecer nenhuma informação útil para a reconstrução da chave privada correspondente, porém este princípio vale somente para chaves a partir de um certo tamanho. As chaves muito pequenas, de fato, não resistem por muito tempo ao processo de criptoanálise, que é favorecido pela disponibilidade, a baixos custos, de potências de cálculo sempre crescentes (a potência de cálculo de um PC, por exemplo, dobra a cada 18 meses, segundo a tendência dos últimos dez anos) (BUONOMO, 2003, p. 7).

Esclareça-se que, para fins do presente estudo, assume-se que as chaves de um par (pública e privada) sempre tenham sido geradas tomando-se os devidos cuidados, dotadas de um tamanho adequado e capaz de garantir uma efetiva independência entre elas, fator esse que, segundo BUONOMO (2003, p. 7) "é considerado *sine qua non* em termos de segurança do método". Não teria sentido o uso prático de um sistema de criptografia assimétrica que descuidasse de problema tão simples de se evitar. Nessa linha de raciocínio, um sistema de criptografia assimétrica é assumido como possuindo chaves realmente independentes entre si.

A despeito dessa independência e desvinculação das chaves utilizadas, em virtude das propriedades e operações matemáticas implementadas num algoritmo assimétrico, cada uma das chaves complementa inversamente a outra, o que as dota da singular capacidade de fazer com que os dados que uma delas tenha

cifrado, obrigatoriamente tenham que ser decifrados pela outra. Ou seja, o que uma chave do par cifra, obrigatoriamente somente a outra chave do par decifra (e vice-versa).

A respeito das relação entre as duas chaves utilizadas pela criptografia assimétrica, GIUSTOZZI (2003, p. 3) pondera: "na prática, um sistema do gênero é dotado de duas chaves distintas, que são uma o inverso da outra: se uma foi usada para a cifragem, a segunda deve ser usada para a decifragem, e vice-versa". Ponto fundamental desse sistema é que as duas chaves devem ser independentes: ou seja, o conhecimento de uma das duas chaves não deve dar nenhuma informação útil para a reconstrução da outra. Para este autor, o conceito de criptografia de chave pública foi primeiramente apresentado no ano de 1976, nos Estados Unidos, por Whitfield Diffie e Martin Hellman. A base dessa nova técnica está justamente na idéia de que as chaves criptográficas não devem ser únicas, como acontece na criptografia simétrica, como forma de solução para os problemas de gerenciamento de chaves que esse método tradicional apresenta. Por definição, as chaves do novo método assimétrico devem ser duplas, geradas como um par, a fim de que uma seja de caráter perfeitamente público (o ideal do método seria que todas as pessoas do mundo tivessem acesso fácil e irrestrito a essa chave) e outra seja de caráter perfeitamente privado (o ideal do método seria que somente uma pessoa no mundo, seu proprietário, tivesse acesso fácil e irrestrito a essa chave).

BUONOMO assim resume os vários aspectos inerentes a essa técnica da criptografia assimétrica:

> Os princípios sobre os quais se funda a nova criptografia são relativamente simples, porém [...] revolucionários: diferentemente do sistema clássico, no qual a chave é única, existem, aqui, duas chaves de cifragem (ditas, respectivamente, chave direta e chave inversa); cada chave pode, indiferentemente, ser utilizada para cifragem ou decifragem; a chave utilizada para cifragem não pode ser utilizada para decifragem; o conhecimento de uma das duas chaves não fornece nenhuma informação sobre a outra chave (BUONOMO, 2003, p. 7).

Aquele que deseje utilizar-se de um sistema de firma digital pode, assim, munir-se de um par de chaves assimétricas de cifragem, usando um programa informático especial para geração e gestão dessas chamadas chaves de cifragem.

O interceptor ativo, quando consegue fazer a quebra da cifragem, pode não somente alterar o conteúdo daquela mensagem, como inclusive gerar novas,

identificando-se como sendo o mesmo emissor da interceptada, uma vez que, falsificando-se o local de emissão e codificando-se a mensagem com a chave secreta, tornam-se muito fortes as evidências de se tratar de uma informação genuína.

> Para este tipo de situação, criou-se o método de criptografia com chave pública. Através deste artifício, mesmo que se tenha o conhecimento da chave secreta de cifragem, torna-se impossível a alteração de mensagem com o uso dessa chave. Em outras palavras, se a mensagem for cifrada com a utilização da chave pública x, essa mesma chave X não poderá ser utilizada para a decifragem dessa mensagem, pois seu resultado não coincidirá com a informação original. Através desta primeira explicação, podem surgir inúmeras dúvidas a respeito de como funcionaria a criptografia por chave pública, uma vez que a chave utilizada para cifrar a mensagem não é a mesma utilizada para decifrá-la (VOLPI, 2001, p. 13).

Para o autor, o que ocorre é a criação de uma nova chave (privada), ou seja, a comunicação entre dois pontos não fica vinculada ao fato de que ambos tenham conhecimento da mesma chave.

A função inicial imaginada para a chave pública seria sempre a de efetuar a cifragem, ao mesmo tempo em que a sua correspondente chave privada deveria ser usada para efetuar a respectiva decifragem. Em resumo, pode-se dizer que a técnica de criptografia assimétrica foi concebida, inicialmente, para que um número ilimitado de pessoas pudessem enviar dados cifrados, com função de sigilo, para serem lidos por uma só pessoa (aquela que possuísse a chave privada que faz par com a chave pública utilizada para cifragem). Com isso, pretendeu-se eliminar as necessidades de distribuição e gerenciamento de chaves secretas (imperativas na criptografia simétrica), já que as chaves utilizadas para cifragem de mensagens, além de serem específicas para cada pessoa, são também públicas (ou seja, deverão estar sempre acessíveis para toda e qualquer pessoa que delas venha a precisar).

De acordo com KALINSKI JÚNIOR & BURTON (2003, p. 7), "os usuários dessa nova técnica de criptografia simplesmente precisam gerar sua chave privada, de acordo com a qual será automaticamente gerada uma correspondente chave pública que constituirá o par". Feito isso, basta que a chave pública seja diretamente distribuída a quem se deseje ou, melhor ainda, seja disponibilizada em um repositório de chaves (*key repository*), situado em local público de fácil acesso para qualquer pessoa (um local acessível via Internet, por exemplo). Não há necessidade

de nenhum cuidado com o sigilo da chave pública, bastando que se mantenha absolutamente secreta a chave privada.

Tal concepção, referente ao uso de uma chave pública e outra privada, foi, sem dúvida, uma grande revolução no campo da criptografia. Não foi só essa, contudo, a valiosa contribuição dessa relativamente recente técnica de criptografia assimétrica, conforme será demonstrado no subtópico a seguir.

Para KALINSKI JÚNIOR & BURTON (2003, p. 37), "tudo o que for cifrado utilizando-se uma chave pública, somente poderá ser decifrado utilizando-se a respectiva chave privada que com ela faça par". O autor comenta que essa foi a intenção de uso inicial do método conforme já explicado. Ocorre, porém, que logo começou-se a observar os efeitos de um uso invertido do par de chaves. Ou seja, não se fazer o uso tradicional de cifrar com a chave pública de uma pessoa, para que ela decifrasse com sua chave privada mas, sim, cifrar-se com a própria chave privada para que qualquer um pudesse decifrar com a respectiva chave pública do par. Isso é perfeitamente possível, pois sabe-se que aquilo que uma chave privada cifra, sua respectiva chave pública decifra e vice-versa. Não demorou para que se tivesse a percepção de que essa simples inversão no uso das chaves poderia trazer um resultado extremamente útil.

KALINSKI JÚNIOR & BURTON abordam a funcionalidade dessa técnica, ressaltando importantes características dessa nova forma de "assinatura" que se vislumbra:

> Um algoritmo de assinatura é um algoritmo que transforma uma mensagem de qualquer comprimento e uma chave privada em uma assinatura, de tal modo que seja computacionalmente não realizável encontrar duas mensagens com a mesma assinatura, encontrar uma mensagem com uma assinatura pré-determinada ou encontrar a assinatura para uma mensagem sem utilizar a chave privada (KALINSKI JÚNIOR & BURTON, 2003, p. 38).

Em síntese, em relação à "assinatura" do documento, a técnica de criptografia assimétrica permite que um emitente possa enviar dados "assinados" (entenda-se, possibilitando aos destinatários certificarem-se de que o emitente realmente é o autor) para um número ilimitado de pessoas (todos aqueles que tenham acesso à chave pública que faz par com a chave privada utilizada para a cifragem).

KALINSKI JÚNIOR & BURTON (2003, p. 37) comentam que essa assinatura "é oriunda de uma dedução", embasada na maneira como se produzem os dados cifrados e na maneira como se decifram tais dados (ou seja, decorre da opção de uso da chave privada para cifrar, que obriga ao uso da chave pública para decifrar). Como resultado da cifragem feita dessa forma, nada mais se tem do que dados em estado normal vertidos para dados em estado cifrado (como, aliás, qualquer técnica criptográfica normalmente cuida de fazer). A possibilidade de verificar a existência da "assinatura" reside exclusivamente da necessidade de uso de uma chave pública de alguém, para fazer-se a decifragem de uma mensagem recebida.

Portanto, não se deve entender a "assinatura" aqui referida como algo que se constitua em algum dado novo que venha a ser inserido – seja em momento anterior ou posterior à cifragem – no conteúdo da mensagem. A "assinatura" nada mais é do que uma presunção, que deriva da forma como é feita a cifragem e a correspondente decifragem (forma essa que reside no simples uso invertido das chaves, em relação ao uso que inicialmente havia sido concebido).

3.3. DOCUMENTOS ELETRÔNICOS BASEADOS NO MODELO "FIRMA DIGITAL/ AUTORIDADE CERTIFICADORA

Neste tópico aborda-se o modelo adotado por diversos países para certificação dos documentos eletrônicos e sua assinatura digital baseada no técnica de criptografia assimétrica. Assim sendo, ressalta-se o Modelo " Firma Digital / Autoridades Certificadoras" e a Aposição de uma Firma Digital sobre um Documento Eletrônico

3.3.1. Modelo " Firma Digital / Autoridades Certificadoras"

Neste momento do presente estudo, para elucidação do funcionamento e da viabilidade prática atual dos documentos eletrônicos juridicamente válidos, utilizaremos o chamado modelo "Firma Digital / Autoridade Certificadora" (*Digital Signature / Certification Authority*).

Tal modelo se baseia na técnica de criptografia assimétrica ou de chave pública, a mesma que vem sendo utilizada, na prática, pelos países que têm acolhido legalmente tal espécie de documento. Na verdade, há que se dizer que, em relação a muitos desses países, em função de uma opção pelas neutralidades tecnológica e técnica das leis editadas acerca da matéria, não há, propriamente, uma adoção legal explícita do modelo citado.

Assim, por exemplo, a lei não menciona o uso da "firma digital" (vinculada à criptografia assimétrica) mas, sim, de "firma eletrônica" (técnica e tecnologicamente neutra), cuidando, apenas, de estabelecer o que deva ser garantido com seu uso (com vistas à obtenção de documentos eletrônicos juridicamente válidos). Ocorre que, ante a inexistência hodierna de outro modelo mais apropriado, acaba-se fazendo uso prático do modelo "Firma Digital / Autoridade Certificadora", pois é somente através dele que os requisitos legais encontram maneira de serem atendidos. Em termos genéricos, tais requisitos, são assim descritos por BUONOMO:

> Para que um sistema criptográfico possa ser corretamente utilizado para a transmissão dos atos ou documentos por via telemática é necessário – de fato, que ele seja capaz de garantir (analogamente à garantia que oferece, hoje, o envio postal em um pacote fechado) a inviolabilidade da correspondência (*confidencialidade*), a conformidade da duplicação transmitida ao original do documento (*integridade dos dados*), a efetiva proveniência do documento daquele que aparece como emitente (*autenticação*), além do assim chamado *não repúdio* (aquele que transmite não deve poder negar ter transmitido, assim como aquele que recebe não deve poder negar haver recebido) (BUONOMO, 2003, p. 3).

Em relação aos estudiosos da matéria, pode-se dizer que há uma situação semelhante ao que ocorre com a legislação dos países. Há os que preferem analisar os documentos eletrônicos sob um ponto-de-vista mais neutro, delineando-o de forma genérica e sem apego a nenhuma técnica ou tecnologia específica (normalmente, são estes os que preferem, usar o termo "firma eletrônica" e não, especificamente, "firma digital"). Tratam-se de abordagens mais conceituais e abstratas. Por outro lado, há os estudiosos que, já de início, elaboram seus trabalhos com uso maciço de referências à criptografia assimétrica, à firma digital, às Autoridades Certificadoras e todos os elementos deste modelo que o presente capítulo se propõe a abordar. São, portanto, abordagens mais concretas e práticas.

Porém, assim como acontece em relação aos países, ambos os grupos de estudiosos acabam se baseando, ainda que uns de forma implícita e outros de forma explícita, na criptografia assimétrica e, consequentemente, no modelo "Firma Digital / Autoridade Certificadora".

Dentro do contexto atual, quando se trata do uso prático de documentos eletrônicos juridicamente válidos, o modelo ora apresentado, segundo BUONOMO (2003, p. 4) "é o único conhecido e tido como confiável". Isso não significa, necessariamente, que ele seja o único possível, pois, com as novas técnicas e tecnologias que vão surgindo, outros modelos logo deverão poder ser implementados na prática. No momento, contudo, por ser essa a melhor forma prática conhecida de implementação dessa nova espécie de documentação, o modelo "Firma Digital / Autoridade Certificadora" demonstra ser o recomendado. Daí, justamente, decorre a importância de se conhecê-lo em maiores detalhes.

3.3.2. Aposição de uma Firma Digital Sobre um Documento Eletrônico

Uma firma digital, conforme RAGOZZO & GIAQUINTO (1997, p. 64) "é obtida como resultado da aplicação da chave privada, de um método de criptografia assimétrica, sobre o conteúdo de um documento eletrônico qualquer". Os autores argumentam que a firma digital é "aposta" em um sentido diferente do usado para a aposição de uma assinatura ou firma tradicional. No caso da firma digital, a aposição se refere ao fato dela ser calculada em função do conteúdo de um determinado documento eletrônico.

Observe-se que uma assinatura tradicional tende a ser, quando se observa vários documentos assinados pela mesma pessoa, sempre, muito parecida. Essa "quase igualdade", apresentada pela assinatura tradicional, é que faz com que ela cumpra a função maior que dela se espera. No caso da firma digital, contudo, é exatamente o fato dela ser completamente diferente, para cada documento, que lhe dá confiabilidade.

RAGOZZO & GIAQUINTO (1997, p. 64) afirmam que "depois de haver redigido o documento com o computador, sempre com o uso do computador, utiliza

a sua 'chave secreta' (similarmente a uma matriz de um selo) para anexar os caracteres de identificação ao final do documento". Para estes autores os caracteres dependerão da chave secreta e do conteúdo do documento, e resultarão, consequentemente, diferentes a cada vez. O controle de validade se efetua por meio do computador, com auxílio da 'chave pública' correspondente, que todos possuem – ou, ao menos, deveriam – possuir.

Assim, tem-se que, enquanto o exame da assinatura tradicional se destina basicamente à verificação da autoria (garantir a possibilidade da imputação subjetiva do documento tradicional que a porta), o exame da firma digital não só garante a autenticidade, mas também garante a integridade do documento eletrônico sobre o qual ela tenha sido calculada. Como ela se vincula a um e tão-somente um documento eletrônico (possuidor de um conteúdo específico), não há maneira de reutilizá-la, ou seja, de extrair a firma digital do documento eletrônico "X" e copiá-la no local onde deveria estar a firma digital do documento eletrônico "Y".

CAMMARATA, sobre a novidade da função de "auto-certificação" cumprida pela firma digital, assim se posiciona:

> [...] complexa e, ao mesmo tempo, [...] significativa, é a questão da aplicação dos procedimentos tradicionais aos documentos e firmas digitais, e não somente no campo processual. Aqui é necessária uma compreensão não superficial dos aspectos técnicos da matéria e, em particular, do formidável mecanismo de 'auto-certificação' dos documentos formados e transmitidos com sistemas informáticos e telemáticos. De fato, a aposição da firma digital [...] torna imediata e completamente automática a verificação da originalidade, da atribuição a um determinado sujeito e do momento da formação e/ou transmissão de um documento (CAMMARATA , 2003, p. 91).

Uma vez que a firma digital é resultado de um cálculo matemático complexo efetuado sobre dados digitais (as já conhecidas seqüências de *bits*), sua criação somente pode ser feita mediante o uso de um sistema apropriado, que compreende o uso conjugado de um computador e um *software (*de criptografia assimétrica). Da mesma forma, a verificação da validade da firma digital, para configuração de todos os efeitos jurídicos que lhe devem ser próprios, somente poderá ser feito através do mesmo uso conjugado de computador e *software*.

A criação da firma digital compreende as atividades de seu cálculo e anexação ao documento eletrônico que será firmado, ao passo que a atividade de verificação (autenticação) consiste na conferência que o computador fará para ver

ser o documento eletrônico provém mesmo do autor nele indicado, e se não ocorreram quaisquer adulterações de conteúdo.

A anexação da firma digital, de acordo com RAGOZZO & GIAQUINTO (1997, p. 64) "é decorrente de uma forma prática de implementação, especificamente a que se utiliza de um resumo do documento eletrônico para, sobre ele, efetuar a aposição da firma digital". Em função da utilização desse resumo é que a firma digital precisará ser anexada ao documento eletrônico. Para este autor, os requisitos essenciais para a validade jurídica dos documentos eletrônicos consistem na garantia de integridade, a garantia de autenticidade e a garantia de tempestividade.

Dentre eles pode-se dizer que a garantia de integridade depende, segundo RAGOZZO & GIAQUINTO (1997, p. 64) "direta e exclusivamente, da aposição de uma firma digital (por isso, pode-se dizer que, para sua verificação, depende-se somente de elementos intrínsecos ao próprio documento eletrônico em si)". O autor comenta sobre a garantia de autenticidade ressaltando que esta decorre da aposição da firma digital mas, também, da existência de uma estrutura capaz de implementar alguns procedimentos imprescindíveis em relação às chaves (as "Autoridades Certificadoras" e, por isso, pode-se dizer que, para sua verificação, depende-se de elementos extrínsecos ao documento eletrônico).

Quanto ao terceiro requisito, a garantia de tempestividade, RAGOZZO & GIAQUINTO (1997, p. 64) diz que "também se vale, diretamente, da aposição de uma firma digital sobre o documento eletrônico". O autor ressalta que não significa, todavia, que qualquer documento eletrônico, ainda que não portador, em si, de firma digital, não poderia, teoricamente, beneficiar-se desse tipo de garantia. No caso da garantia de tempestividade, assim como ocorre com a garantia de autenticidade, há necessidade da existência de uma estrutura capaz de implementar alguns procedimentos imprescindíveis para se datar os documentos eletrônicos (o chamado "selo cronológico digital" e, por isso, há uma dependência de elementos extrínsecos ao conteúdo do documento eletrônico em si).

As garantias de integridade e autenticidade serão comentadas em subtópicos a seguir. A garantia da tempestividade será comentada em tópico próprio, mais adiante. Se, por outro lado, pensar-se em efetuar o cálculo, com uso da chave privada, sobre o inteiro teor do documento, então a firma digital não precisaria ser

anexada. Essa criação do resumo tem, basicamente, fins de economia de tempo de processamento na execução das tarefas de criação e autenticação da firmas digitais dos documentos eletrônicos. Em tópico referente ao uso prático das firmas digitais, mais adiante, ficará mais claro como funciona esse resumo.

a) Garantia de Integridade

Sobre a integridade garantida a um documento eletrônico com firma digital, muito pouco resta a dizer. A forma como ela é obtida já foi explicada. Basta ressaltar que todos os elementos necessários à verificação da integridade de um documento eletrônico, portador de firma digital, encontram-se em seu próprio conteúdo. Nesse sentido, a verificação, conforme MARCACINI (2003, p. 11), "é interna, pois necessita, apenas, de elementos que são intrínsecos ao próprio documento eletrônico portador de firma digital".

Isso significa que, cada vez que esse documento eletrônico seja duplicado, todos esses elementos estarão presentes na nova duplicação. Em função disso, diz-se duas coisas: primeiro, que cada duplicação é um novo original (e não uma mera cópia), pois é exatamente idêntica ao documento eletrônico que lhe serviu de matriz. Segundo, que o conteúdo de um documento eletrônico com firma digital, por si só, é "auto-certificável", ou seja, não depende, para confirmação de sua integridade, do suporte informático (suporte material) onde esteja. Sobre o nível de integridade proporcionada a um documento eletrônico pela aposição de uma firma digital, afirma MARCACINI:

> Assinado um documento eletrônico – o que é feito com o uso da chave privada –, é possível conferir a assinatura mediante o uso da chave pública. E, além disso, ao efetuar a assinatura, o programa, utilizando fórmulas matemáticas sofisticadas, *vincula a assinatura digital ao documento assinado*, de tal sorte que a assinatura digital só seja válida para aquele documento. Qualquer alteração, por menor que seja, na seqüência de bits que forma o documento eletrônico, invalida a assinatura. A simples inserção de mais um espaço entre duas palavras, não obstante o sentido do texto não ter sido modificado, já é bastante para que seja perdido o vínculo com a assinatura digital (MARCACINI, 2003, p. 14)

Portanto, é impossível alterar-se, de forma imperceptível, o conteúdo de um documento eletrônico portador de firma digital. Qualquer alteração, ainda que fosse, por exemplo, a substituição de um "a" por um "A", de um ponto por uma vírgula, a

inserção de uma linha em branco ou qualquer outra alteração que fosse, resultaria no desaparecimento da possibilidade de auto-certificação. Ou seja, durante a autenticação efetuada sobre um documento eletrônico desses, que tenha sofrido adulteração, o resultado será negativo. Isso decorre, em termos práticos, do fato de que as operações matemáticas efetuadas no processo de conferência da firma digital não possuírem mais um resultado válido. Como a seguinte operação expressasse a sua criação: 2 x 3 = 6, sendo que 2 é a variável "chave privada", 3 é a variável "conteúdo do texto" e 6 é o resultado da operação, ou seja, a "firma digital" calculada. Imagine-se que, em um dado momento, ocorresse uma mudança no conteúdo do texto. Suponha-se que este passe a ser 4 (em vez de 3, como era originalmente). Na atividade de autenticação desse documento eletrônico, a operação matemática se apresentaria assim: 2 x 4 = 6. Ou seja, ocorreu uma perda de sentido lógico, já que o resultado (firma digital) não confere com as variáveis que a deveriam ter produzido. Por isso, seguramente, o *software* que faz a autenticação poderá ter certeza de que houve uma adulteração (no caso, da variável "conteúdo do texto").

Num exemplo bem simples, sabendo-se que a firma digital é calculada com base em duas variáveis, suponha-se que decorrência dessa autenticação negativa, pode-se dizer que a firma digital perde sua validade e, por conseguinte, o documento torna-se apócrifo. Com isso, se vê que a perda de integridade aniquila também com a autenticidade do documento.

Importante deixar claro, contudo, que a garantia de integridade não se refere à existência de qualquer impossibilidade prática de efetuar alterações, em si, sobre o conteúdo de um documento eletrônico portador de firma digital. Como tais documentos são compostos por dados digitais, eles não são indeléveis, mas sim facilmente alteráveis. AUGUSTO (1993, p. 35) comenta que "o mecanismo de garantia da integridade fornece uma forma imediata e plenamente segura de detecção das adulterações, não visando, propriamente, impedir a sua realização".

MARCACINI (2003, p. 02) em relação ao tema, pondera: "as assinaturas digitais assim produzidas ficam de tal sorte vinculadas ao documento eletrônico 'subscrito' que, ante a menor alteração, a assinatura se torna inválida". A técnica não

só permite demonstrar a autoria do documento, como estabelece uma 'imutabilidade lógica' do seu conteúdo.

> Por 'imutabilidade lógica' quero dizer que o documento continua podendo ser alterado, sem deixar vestígios no meio físico onde está gravado (esta, aliás, é uma importante característica do documento eletrônico, que vai permitir desvinculá-lo do meio físico e transmiti-lo, via Internet); entretanto, a posterior alteração do documento invalida a assinatura, o que faz com que o documento deixe de ter valor como prova (MARCACINI, 2003, p. 02).

Acerca dos aspectos importantes da garantia da integridade dos documentos eletrônicos, ZAGAMI afirma que:

> No que se refere a outro ponto – além da imputabilidade – sobre o qual se funda a eficácia probatória de um documento, e que vem a ser a possibilidade de verificação de sua integridade, tradicionalmente confiada à materialidade do suporte, observe-se que a firma digital não permite a criação de documentos indeléveis, mas permite, em vez disso, reconhecer eventuais alterações que tenha sofrido o conteúdo do documento, a partir do momento em que lhe seja aposta a respectiva firma digital (ZAGAMI, 2003, p. 4).

Qualquer modificação, seja de um só *bit*, seja acidental, seja intencional, do documento eletrônico firmado, seja ele um texto, uma imagem, um som, é fácil e rapidamente verificável. E, isso, sem a necessidade de recorrer-se a complicadas e incertas análises científico grafológicas

b) Garantia de Autenticidade

A firma digital é composta com base no conteúdo do documento eletrônico e, em si mesma, não apresenta nenhuma relação com o aquela pessoa que o esteja produzindo. Por isso é que pode-se dizer que, na maioria dos casos, a autenticidade dependerá, para sua verificação, de algum elemento extrínseco ao conteúdo do documento eletrônico portador de uma firma digital. Diz-se "na maioria dos casos" porque, conforme já se sabe, no caso de adulteração no conteúdo (perda de integridade), a firma digital resulta invalidada e, consequentemente, o documento perde sua autenticidade. A verificação da autenticidade, conforme ROGNETTA (2003, p. 2) "dependerá de elementos extrínsecos sempre que houver integridade". Na falta desta, através dos próprios elemento intrínsecos do conteúdo de um

documento eletrônico portador de firma digital, restará aniquilada também a autenticidade.

ROGNETTA aborda as questões envolvidas com a verificação da autenticidade de um documento eletrônico portador de firma digital:

> Com efeito, o problema que se apresenta com o uso da criptografia assimétrica é o seguinte: se recebo um ato via correio eletrônico, contendo uma firma digital aposta, e o procedimento de verificação sobre a mesma resulta positivo, tenho a certeza de que o documento provém daquele que resulta ser o emitente da chave pública. Mas, se o emitente for qualquer um que se faça passar por outra pessoa, como faço eu para controlar? Ou, todavia, se também estou certo da identidade do emitente, como posso verificar que ele é plenamente capaz de entender e de manifestar sua vontade? E se aquele que resulta ser o emitente do ato negar ser o titular da chave privada? (ROGNETTA 2003, p. 2).

O autor ressalta que para resolver estes problemas, intervêm no sistema as autoridades certificadoras, que podem suprir as óbvias carências do computador em matéria de controle sobre a plena subsistência dos direitos e sobre a capacidade em relação à conclusão dos atos jurídicos. Em todo caso, é bom sublinhar que o eventual controle para fazer frente a esses quesitos acima citados seria muito mais simples do que aquele necessário em caso de contestação sobre uma assinatura de um documento tradicional em papel.

MICCOLI (2003, p. 9) argumenta que, embora todo o sofisticado aparato tecnológico que se possa colocar a serviço do sistema, "não será possível jamais garantir que a firma digital tenha sido aposta pelo legítimo titular e não, por exemplo, por sua secretária ou qualquer outra pessoa que, ilegitimamente, o tenha feito". Segundo o autor, através de mecanismos de responsabilização civil, sempre será garantido à parte lesada o direito de obter ressarcimento dos danos, o que impeliria os titulares de chave privada, numa atitude preventiva, usarem máxima cautela na guarda de suas chaves privadas. No entanto, isso pode não ser o suficiente, pois o simples ressarcimento de danos nem sempre cumpre o mesmo papel da efetiva obtenção do direito original.

As questões que se impõem, a respeito da autenticidade de um documento eletrônico portador de firma digital, portanto, são um pouco diferentes daquelas envolvidas na verificação de sua integridade. Enquanto, para verificação desta última, tudo o que é preciso encontra-se no próprio conteúdo do documento eletrônico portador de firma digital, na verificação da autenticidade, alguns

elementos da verificação são externos. MICCOLI (2003, p. 10) relata que o problema fundamental da autenticidade de uma firma digital "é saber se, efetivamente, o titular da chave privada utilizada em sua criação é, realmente, quem diz ser". De acordo com o que até aqui tem sido exposto, a verificação da autenticidade de um documento eletrônico decorre, basicamente, do uso da chave pública de alguém, para decifragem de um conteúdo qualquer, que tenha sido cifrado pela respectiva chave privada.

Se a decifragem obtiver sucesso, isso significa que as chaves utilizadas (a privada, para cifragem, e a pública, para decifragem) formam um par. Se o par existe, uma pessoa está vinculada a ele, pois, alguém providenciou a emissão desse par de chaves. Como saber quem foi?

Uma chave pública, supondo-se que esteja em um repositório de chaves acessível via Internet, possuirá o nome da pessoa que é sua proprietária associado a ela. Porém, se o processo de emissão desse um par de chaves foi algo feito sem qualquer controle, quem garante que o nome associado à chave pública é, realmente, da pessoa que providenciou a emissão do par? O que impediria Paulo de emitir um par de chaves em nome de João e, posteriormente, sair por aí aplicando firmas digitais em documentos eletrônicos como se isso fosse feito pelo próprio João?

Em virtude de tais problemas, já se pode observar que há necessidade de procedimentos destinados a gerenciar a emissão e, mesmo, o próprio uso das chaves assimétricas. Sem isso, um documento eletrônico portador de firma digital não teria como apresentar uma autoria certa e comprovável. É por isso que o modelo se chama "Firma Digital / Autoridade Certificadora". Esse segundo componente, a Autoridade Certificadora, é que estará encarregada do mencionado gerenciamento.

BUONOMO aborda aspectos relativos ao tema:

> É de toda evidência que a identificação de quem efetua o depósito da chave pública, que será utilizada para decifrar a firma aposta com a correspondente chave privada, é de importância decisiva para o fim do correto funcionamento do sistema inteiro. [...] Em extrema síntese, então, o sistema funciona com a condição de que a chave pública seja 'certificada' e que o par inseparável de chaves seja de tamanho (calculado em *bits*) adequado para garantir uma suficiente *robusteza computacional* no que se refere à potência de cálculo disponível (BUONOMO, 2003, p. 4).

É por este motivo, que o regulamento [Lei italiana 59/97, de 15.03.97, que regula o uso de documentos eletrônicos no âmbito da Administração Pública italiana] confia ao 'procedimento de certificação' a validade do processo inteiro.

As chaves assimétricas de cifragem têm uma duração limitada e podem ser suspensas ou revogadas por seu titular (analogamente ao que ocorre, sob outra forma, com os cartões de crédito). BUONOMO (2003, p. 4) argumenta que "o depósito da chave pública deve ser efetuado junto a um sujeito capaz de assegurar a correta manutenção do sistema de certificação e – em particular – capaz de garantir o acesso telemático aos registros das chaves públicas".

Em decorrência da importância assumida pelas chamadas Autoridades Certificadoras para a operacionalização do modelo que está sendo descrito, é sobre elas que se trata no tópico a seguir.

c) As Autoridades Certificadoras (Cibernotários)

A denominação "Cibernotário", refere-se, de acordo com MICCOLI (2003, p. 11), "a um notário atuando no ciberespaço, ou seja, a quem, no ambiente virtual das redes telemáticas (como a Internet), possua funções de objetivos similares (mediante as devidas adaptações) àquelas exercidas pelos notários tradicionais. O termo "Autoridade Certificadora", por sua vez, possui um significado mais genérico do que o termo "Cibernotário", podendo ser aplicado tanto a entidades públicas quanto privadas. O segundo termo se apresenta mais ligado a entes públicos, governamentais. No âmbito do presente trabalho, adota-se o uso do termo "Autoridade Certificadora", justamente em razão do mesmo ser mais neutro (ou seja, permitindo entender-se uma Autoridade Certificadora como sendo uma entidade qualquer, que possua os atributos legais necessários à execução de suas funções, não estando preestabelecido que deva tal entidade ser pública, mas, ao mesmo tempo, não se excluindo tal possibilidade).

A necessidade das Autoridades Certificadoras prende-se, diretamente, à necessidade de se implementar um mecanismo, uma infra-estrutura, capaz de possibilitar uma forma confiável de verificação de autenticidade dos documentos

eletrônicos portadores de firma digital. MICCOLI, a respeito da importância destas Autoridades Certificadoras, afirma que:

> É de imediata evidência que a função das autoridades certificadoras se reveste de uma importância e uma delicadeza essencial dentro do sistema delineado [documentos eletrônicos juridicamente válidos], tanto que o sistema de cifragem por chaves assimétricas tem sido mais justamente descrito como *Digital Signature / Certification Authority Infrastructure*, ou sistema de firma eletrônica a chave assimétrica submetido a uma autoridade certificadora (MICCOLI, 2003, p. 11).

MARCACINI, sobre a função primordial das Autoridades Certificadoras, ou Cibernotários, assim se manifesta:

> Em primeiro lugar, importa distinguir que as funções do cibernotário serão de certificar a autenticidade da chave pública, e não do documento eletrônico. De posse de uma chave pública sabidamente autêntica, qualquer um, com o uso do *software* correspondente, poderá conferir a autenticidade do documento eletrônico, inclusive o próprio juiz da causa, pessoalmente (MARCACINI, 2003, p. 22).

Para efetuar a verificação de uma firma digital, o interessado deve ter acesso à chave pública do signatário, ao mesmo tempo em que deve estar seguro de que ela faça par com a chave privada desse signatário (ou seja, aquela usada na criação da firma digital). Contudo, um par de chaves assimétricas, uma pública e outra privada, nada mais é do que um amontoado de *bits*, que não se vinculam, por si só, com uma determinada pessoa.

Portanto, um mecanismo adicional é necessário para criar o indispensável liame entre as chaves assimétricas e uma determinada pessoa, titular do poder de seu uso. Tal mecanismo é implementado através da criação das chamadas Autoridades Certificadoras, as quais devem possuir o atributo de serem terceiros neutros, que gozem da confiança de todos (as chamadas *Thrusted Third Party*366). FROOMKIN (2003, p. 5) define Autoridade Certificadora como "um ente, seja público ou privado, que busca preencher as necessidades de serviços de thrusted third party [...], através da emissão de certificados digitais que atestam alguns fatos sobre o sujeito do certificado".

As Autoridades Certificadoras desempenham papel fundamental, de muitas atribuições, dentro do modelo que ora se está comentando. A primeira e, talvez, principal delas, é relacionada com a atividade de emissão do par de chaves assimétricas. Para FROOMKIN (2003, p. 5) "é da Autoridade Certificadora a

incumbência de dar credibilidade ao par de chaves possuído por uma determinada pessoa". Para tanto, qualquer pessoa que pretenda possuir seu par de chaves, devidamente certificado, deverá submeter-se a um procedimento minucioso de avaliação e conferência de sua identidade, antes de recebê-lo.

> Conforme consagrado internacionalmente, as chaves de identificação são concedidas por Autoridades Certificadoras ou Certification Authorities. As autoridades certificadoras, em regra, são empresas privadas encarregadas de averiguar a identidade de pessoas para fins de emissão de uma espécie de identidade eletrônica, no intuito de possibilitar a realização de operações identificadas nas redes de computadores (LIMA NETO, 2003, p. 7).

Devido à importância de suas funções, um dos pontos de maiores estudos dentro do modelo "Firma Digital / Autoridade Certificadora" tem sido, justamente, o estabelecimento de parâmetros para determinação do perfil adequado exigível de quem pretenda assumir o papel de Autoridade Certificadora. De certo e incontestável, tem-se que tal entidade deve assumir uma posição de absoluta neutralidade entre as partes, ou seja, deve ser uma parte que goze da confiança de todos, não possuindo quaisquer interesses outros que não, pura e simplesmente, exercer aquelas atividades afetas a uma Autoridade Certificadora. Sobre as dificuldades da tarefa de definição sobre quem estaria apto a tal papel, assim se manifesta MICCOLI:

> A autoridade certificadora, entendida como *Thrusted Third Party*, como terceiro, ou seja, que goze de incondicionada confiança das partes contraentes é, talvez, o conceito sobre o qual mais se debruçaram os técnicos e os juristas americanos, buscando individualizar quem possa preencher adequadamente tal papel. É evidente, de fato, que a individualização de um terceiro que não goze da confiança dos usuários do serviço de comércio eletrônico poderia invalidar gravemente o desenvolvimento desse tipo de comércio (MICCOLI, 2003, p. 13).

Existem, na opinião do autor acima citado, duas formas de se conceber as Autoridades Certificadoras. A primeira forma, mais flexível, permite que uma ampla gama de entidades assumam e desempenhem tal papel, impondo-lhes o cumprimento de algumas obrigações e deveres. Nos Estados Unidos, por exemplo, as legislações estaduais (o próprio pioneiro *Utah Digital Signature* Act, por exemplo), adotam essa posição de flexibilidade. O Estado, nesse caso, ficaria no papel de regulamentador e fiscalizador do exercício da atividade. A segunda forma, mais rígida, tende a restringir a atividade ao âmbito de órgãos do próprio Estado, dotados de fé pública, sendo as Autoridades Certificadoras, aqui, entendidas bem aos

moldes dos conhecidos notários (os quais, especificamente, devido à modernidade do tema, são chamados de Cibernotários). Seguindo tal pensamento encontram-se, por exemplo, a Itália e o Canadá. A seguir, apresenta-se o pensamento de alguns estudiosos, acerca do tema da definição de quem poderia exercer melhor o papel de Autoridade Certificadora.

Autoridade Certificadora desempenha dentro do sistema, posicionando-se: "Não por acaso, as pesquisas encaminham-se no sentido de dotar o ato de conferência das chaves aos interessados de caráter oficial e público, exercido com independência, um T.T.P. (*Thrusted Third Party)*, um terceiro que possa gozar da confiança das partes que contratem eletronicamente e tenham necessidade de obter o par de chaves para aposição de sua assinatura digital.

MARCACINI faz ressalva de que a função, apesar de importante, não necessita ser desempenhada, obrigatoriamente, por uma entidade estatal, citando exemplos de algumas entidades privadas que também poderiam cumpri-la:

> É de se dizer, ainda, que a função de certificar chaves públicas pode bem ser desempenhada por outros entes, que não o nosso tradicional tabelião. Não seria demais imaginar que a Ordem dos Advogados, por exemplo, mantenha cadastradas as chaves públicas dos advogados; o Poder Judiciário, as dos juizes; bancos e instituições de crédito podem arquivar as chaves públicas de seus clientes, reconhecidas por estes últimos em documentos físicos assinados manualmente. Mesmo faltante a fé pública de quem certifica a chave pública, a autenticidade desta poderá ser comprovada pela exibição da ficha em papel, em que o usuário pessoalmente reconheceu a chave pública como própria (MARCACINI, 2003, p. 22).

Apesar das divergências entre os estudiosos, sejam quais forem as entidades habilitadas a exercerem o papel de Autoridades Certificadoras, contudo, uma unanimidade já se pode constatar: trata-se do entendimento de que tais entidades devam, obrigatoriamente, estar na posição de *Thrusted Third Party*. RAGOZZO & GIAQUINTO expõem opinião nesse sentido, demonstrando, ainda, sua preferência pelo desempenho da atividade por um órgão público:

> É essencial, para os fins de uma tutela jurídica, que as chaves públicas sejam custodiadas por uma autoridade acima das partes, diversa dos sujeitos que participam da relação jurídica. A garantia da autenticidade das chaves públicas poderia ser dada por uma autoridade estatal (tribunal, câmara de comércio, etc.) ou supranacional, ou por oficiais públicos, os quais poderiam ser os notários. Quem quer que pretendesse difundir seus documentos firmados eletronicamente, depositaria junto a uma autoridade a sua chave pública, de modo que essa possa sempre ser verificada por terceiros (RAGOZZO & GIAQUINTO, 2003, p. 8).

Atualmente, no mundo, existem determinadas empresas que, conforme RAGOZZO & GIAQUINTO (2003, p. 8), "ao mesmo tempo em que são produtoras de *software* de criptografia, mantêm um serviço que pretende suprir as funções de uma Autoridade Certificadora". Os autores comentam que isso começou, inicialmente, devido ao fato de não haver o acolhimento oficial dos documentos eletrônicos juridicamente válidos pelo ordenamento de nenhum país. Sendo assim, como primeiro foram desenvolvidas a técnica e a tecnologia (relativa ao modelo objeto do presente capítulo), alguém teve que desempenhar tal função. E foram algumas das próprias empresas de *software*, para viabilizarem seu produto, que assumiram tal tarefa. Agora, contudo, quando muitos países estudam o modelo e estão em vias de adotá-lo, dá-se o questionamento acerca do desempenho do papel por essas empresas de *software*.

A principal razão seria a sua falta de neutralidade. MICCOLI (2003, p. 14), afirma que "a posição de terceiro da Autoridade Certificadora deve manter-se não somente em relação às eventuais partes mas, também, em relação ao sistema técnico que garante o serviço".

Com isso, o autor quer descartar a participação, em tal atividade, dos produtores de *software* ou de outros aparatos técnicos utilizados na implementação do modelo que dá suporte à firma digital (e, consequentemente, aos documentos eletrônicos juridicamente válidos). Teme-se que os interesses comerciais possam macular a posição de neutralidade que, obrigatoriamente, se idealiza para uma Autoridade Certificadora. Imagine-se, por exemplo, que a Autoridade Certificadora constate que o sistema técnico por ela utilizado não está apresentando o funcionamento adequado, possuindo alguma falha de segurança ainda não detectada. Sendo essa Autoridade Certificadora a produtora do tal sistema técnico, ela poderá ficar tentada a não divulgar o problema, causando riscos a todos apenas para preservar seus interesses comerciais.

Por outro lado, sendo tecnicamente neutra e não visando rendas e objetivos diversos, a Autoridade Certificadora tenderá a ter, sempre, em virtude da responsabilidade que sobre ela pesará, o interesse de sanar, imediatamente, quaisquer problemas verificados com o sistema técnico por ela adotado. Além disso, uma Autoridade Certificadora tecnicamente neutra poderá passar a usar quaisquer

inovações ou melhorias surgidas, sejam quais forem as empresas de *software* produtoras.

MICCOLI argumenta que os problemas de ordem jurídica referentes às Autoridades Certificadoras – no caso, *Cybernotary*, conforme o projeto que estuda a participação dos notários no desempenho de tal papel – podem ser resumidos em:

> a) a *Certification Authority*, sendo responsável e garante do serviço, por unânime consenso dos estudiosos deve ser uma T.T.P. – *Thrusted Third Party*, um terceiro, isto é quem goze de incontestável confiança das partes;
>
> b) para que o comércio eletrônico seja verdadeiramente eficaz, ele deve desenvolver-se em nível planetário; não haveria sentido se o anulamento das distâncias obtido com a quase instantânea transmissão dos dados permitida pelos computadores fosse frustrada porque os diferentes sistemas jurídicos nacionais não permitem o uso global do sistema;
>
> c) quem garante que a *chave privada* seja utilizada pelo legítimo titular e não por outro, quer pela negligência em custodiá-la, quer por um fato fraudulento de terceiro? (MICCOLI, 2003, p. 14).

Especificamente em relação ao item "b" acima citado, o próprio MICCOLI faz ressalva que mesmo em países sem tradição de uso de notários públicos, como é o caso dos Estados Unidos, já estar se estudando a possibilidade de sua criação:

> Se tem pensado que, a fim de aumentar o grau de certeza limitadamente às transações eletrônicas destinadas a envio a países estrangeiros, procura-se introduzir nos Estados Unidos um profissional que, de um lado, fosse dotado dos poderes de certificação [...] conferido ao *Public Notary*, e de outro fosse dotado da cultura jurídica própria de um advogado que tenha superado os exames de admissão ao Bar (*Amercian Bar Association*) e que, além disso, enfrentasse cursos de atualização seja em matéria de informática, seja em matéria notarial (entendida assim aquela de tipo latino) (MICCOLI, 2003, p. 15).

Tal necessidade se torna clara em função do caráter globalizado que as normas sobre os documentos eletrônicos e firmas digitais apresentam. Sendo um documento eletrônico algo de circulação teoricamente ilimitada, desconhecedor de fronteiras – transmissível, em segundos, de um canto a outro do planeta –, imperativa se torna a uniformização de procedimentos e, muitas vezes, até de normas. Com isso, se pretende que um documento eletrônico juridicamente válido seja assim considerado tanto nos Estados Unidos, quanto na Itália; tanto no Brasil, quanto na China ou no Japão. Para tanto, pouco deve importar que o sistema jurídico adotado por qualquer desses países seja a *civil law* ou a *common law*.

Tornou-se claro, ante o exposto, a importância das funções desempenhadas pelas Autoridades Certificadoras. Sendo assim, a todos aqueles que se habilitarem a exercê-la, deverá ser atribuído um conjunto de obrigações muito bem estabelecido, prevendo deveres e sanções à altura das responsabilidades assumidas. MARCACINI, a respeito, afirma:

> [...] evidentemente, a negligência ou o dolo do cibernotário no exercício de suas funções poderão implicar em sua responsabilidade civil e criminal. Mas, para caracterizar negligência, necessário será estabelecer criteriosamente quais as cautelas e procedimentos que se deverá observar ao expedir um certificado de autenticidade de chave pública, ou realizar quaisquer outros atos notariais no mundo virtual (MARCACINI, 2003, p. 24).

Deve ser estabelecido o enquadramento legal e de operação das autoridades competentes para a emissão, armazenamento e validação de certificados eletrônicos. Será possível, deste modo, lançar as bases para a infra-estrutura organizacional e tecnológica necessária para suportar os procedimentos eletrônicos de apoio ao notariado eletrônico. No sentido de demonstrar a amplitude de tais deveres e, ao mesmo tempo, observar-se o que têm pensado os estudiosos, serão transcritas, a seguir, três manifestações pertinentes ao assunto.

MICCOLI (2003, p. 16), sobre o papel das Autoridades Certificadoras, de forma genérica, afirma que: "se tem mencionado a *Certification Authority* como um elemento portador da complexa arquitetura que deverá presidir o desenvolvimento de massa do comércio eletrônico em bases globais". Para o autor, competências primárias da *C. A.* [*Certification Authorities* ou Autoridades Certificadoras] deverão ser: a compilação dos algoritmos de firma digital [observe-se que o termo 'algoritmos', aqui, para a autora, tem sentido idêntico ao das chaves da criptografia assimétrica], a sua distribuição aos usuários, a publicação e a atualização dos elencos de algoritmos destinados a serem públicos [entenda-se: chaves públicas], a retirada dos algoritmos pertencentes a pessoas não mais existentes, sob o plano físico e sob o plano jurídico; a colocação em operação de estratégias que tornem o sistema o mais inatacável em âmbito externo e o mais inviolável em âmbito interno.

É importante ressaltar que a geração e a transmissão da chave devem ser reguladas com muito cuidado. Adotando-se a geração do par de chaves como função da Autoridade Certificadora, há que se adotar procedimentos técnicos capazes de garantir que a chave privada assim gerada não venha a ser exposta a

outras pessoas quaisquer, que não o seu próprio titular. Ou seja, mesmo a Autoridade Certificadora que gerará o par de chaves não deverá ter acesso ao conteúdo da chave privada desse par, não devendo armazená-la em meio de armazenamento permanente dentro de seus computadores, duplicá-la ou, de qualquer outra forma, efetuar qualquer procedimento que possibilite ou facilite que terceiros tenham acesso a essa chave privada gerada.

d) Certificados

A Autoridade Certificadora cumpre sua maior atribuição, eminentemente, mediante a emissão de "certificados" (também chamados de "certificados de autenticidade", em decorrência da função que visam cumprir). A. FROOMKIN (2003, p. 12) define certificado como "uma declaração digitalmente assinada por uma Autoridade Certificadora que fornece confirmação independente de um atributo reivindicado por uma pessoa que oferece uma assinatura digital". O autor comenta ainda que mais formalmente, um certificado consiste num registro baseado em computador que: identifica a Autoridade Certificadora que o emitiu; nomeia, identifica ou descreve um atributo do subscritor; contém a chave pública do subscritor; e, está firmado digitalmente pela Autoridade Certificadora que o emitiu.

A respeito da importância de um certificado, ZAGAMI assim se manifesta:

> A verificação de uma firma digital com a chave pública do subscritor, embora forneça a certeza que o documento não tenha sofrido nenhuma alteração e que possa ser proveniente somente de uma pessoa que conheça a chave privada correspondente, não dará, contudo, por si só, alguma indicação certa acerca da real identidade (nome e sobrenome) desta última pessoa (key legitimacy) (ZAGAMI; 2003, p. 7).

Segundo o autor, qualquer um poderia, de fato, criar o par de chaves, associá-lo a um nome de uma outra pessoa real ou de fantasia – eventualmente inserir a chave em um key repository – e então usar o nome falso e a chave privada correspondente para gerar uma firma digital.

A solução deste fundamental problema é obtida com o sistema de certificados, que vêm a ser documentos eletrônicos que associam uma chave pública a uma certa identidade pessoal, previamente verificada por uma pessoa ou organização autorizada (Certification Authority).

O certificado é, ele próprio, nada mais, nada menos, do que um documento eletrônico portador de uma ou mais firmas digitais (no caso, da ou das Autoridades Certificadoras que lhe conferem garantia). É, o certificado, uma espécie de "carteira de identidade eletrônica" de uma pessoa. Daí, a necessidade de sua ampla garantia de segurança. XEXÉO, a respeito desse aspecto, ressalta que:

> Um certificado é uma prova de identidade fornecida por uma entidade conhecida e confiável, que garante que uma assinatura pertence a entidade que a reclama. Certificados são fornecidos por uma Autoridade Certificadora (AC). As chaves privadas das ACs são de extrema importância e devem ser mantidas em uma Unidade de Assinatura de certificados, uma caixa de alta segurança que destrói seu conteúdo se aberta. Como uma AC pode ser alvo de um ataque intensivo, sua chave deve ser muito longa, provavelmente 1.000 *bits* ou mais (XEXÉO, 2003, p. 6).

Um certificado de autenticidade poderia conter informações juridicamente relevantes, segundo MARCACINI (2003, p. 18) "fazendo com que a assinatura digital contenha um *plus* em relação à assinatura manuscrita". Pode-se pensar, por exemplo, em fazer incluir no certificado que o titular da chave é representante legal de tal ou qual pessoa jurídica, conforme consta dos estatutos sociais exibidos ao Cibernotário. Isto conferiria maior segurança a respeito da capacidade daquele que age em nome de pessoas jurídicas. Como estes certificados deverão especificar o seu prazo de validade – seria temerário produzir-se certificados perpétuos –, espera-se que ao menos dentro deste prazo a pessoa continue a exercer estes poderes de representação; em caso contrário, o certificado ainda poderá ser revogado antecipadamente.

CAMARATA, comentando dispositivo contido em esboço de norma italiana (destinada a regular o uso de documentos eletrônicos no âmbito da Administração Pública italiana), afirma:

> Um outro ponto interessante diz respeito à natureza da assinatura 'eletrônica' (art. 7): nos modos e com as técnicas que estão definidas no emanado Regulamento, da assinatura eletrônica deverá sempre ser possível conhecer: para as pessoas físicas: sobrenome, nome, local e data de nascimento, domicílio e código fiscal – para os sujeitos diversos das pessoas físicas: denominação, sede do sujeito ou ente titular, código fiscal; sobrenome, nome, local e data de nascimento e relação funcional ou de representação da pessoa física consignatária – a data da sua geração aos cuidados da competente autoridade de certificação – o período inicial e final de sua validade – o horário de aposição ao documento ou ao grupo de documentos ao qual se refere a eventual certificação de sua validade [...]. É fácil imaginar quais simplificações poderão derivar de uma aplicação generalizada desta 'carteira de identidade virtual', também em seu uso combinado com os cartões inteligentes [*smart cards*]

> que finalmente começam a difundir-se para os usos mais diversos (CAMARATA, p. 2003, p. 16)

Pode-se dizer que um certificado deverá conter, basicamente: uma chave pública e a identificação da pessoa que seja sua titular (bem como, por conseqüência, essa mesma pessoa será titular da chave privada que com ela faça par), informações sobre a data de validade do certificado (ou seja, a data na qual o certificado e as chaves, em si, expirarão), informações sobre a(s) Autoridade Certificadora(s) que garantem tal certificado e, principalmente, a firma digital dessa(s) Autoridade(s), aplicada sobre todas as informações mencionadas. É neste último elemento, com mais força, que reside a efetiva garantia da autenticidade, dentro do modelo "Firma Digital / Autoridade Certificadora". Isso porque, garantindo-se a autenticidade do certificado, por conseqüência, se está garantindo a autenticidade do documento eletrônico portador de uma firma digital certificada.

Para finalizar este subtópico, cabe fazer uma distinção importante: podem existir firmas digitais certificadas e firmas digitais não-certificadas. As primeiras, são as firmas digitais de que trata o modelo ora analisado. As últimas, apesar de garantirem integridade dos documentos eletrônicos sobre os quais serão apostas, não garantem a autenticidade (porque não há Autoridade Certificadora que tenha certificado o par de chaves sobre o qual tais firmas digitais se fundam). ZAGAMI elabora comentários abrangentes e significativos a respeito do tema:

> Com o sistema de certificação das chaves públicas está superada qualquer distinção entre escritura privada autenticada e não. Na realidade, aquilo que vem autenticado não é mais a assinatura, ou seja, a firma digital; ao contrário, é o certificado, com o qual uma certa chave pública vem combinada com uma certa identidade pessoal verificada pelo notário ou outro oficial público, no modo tradicional [...]. A autenticação se faz em uma fase diferente e anterior, e se exaure em um só ato, válido por uma multiplicidade de firmas digitais (ZAGAMI, 2003, p. 9).

Para o autor acima citado, é possível consequentemente, corretamente distinguir entre: escritura privada com firma digital verificável com chave pública certificada e escritura com firma não certificada. No segundo caso, o documento eletrônico-escritura privada não terá valor probatório, a menos que ele seja reconhecido.

Pode-se não obstante, distinguir um valor probatório diverso em relação ao sujeito de onde tenha provindo o certificado: se provém de um notário ou de um

outro oficial público ou organização para isso autorizada, a firma digital deverá certamente, como uma assinatura tradicional, ser legalmente reconhecida; ao contrário, se o certificado provém de sujeitos diversos, se poderá requerer outros elementos probatórios para verificar a correspondência entre uma certa pessoa e uma certa cópia de chave, admitindo que poderá também ser impossível obter-se plena certeza em todos os casos.

e) Infra-estrutura de Chave Pública

A estrutura organizacional e hierárquica que abriga as Autoridades Certificadoras, comumente nos países de língua inglesa, segundo MICCOLI (2003, p. 17), "é conhecida como Infra-estrutura de Chave Pública (*Public Key Infrastructure*)". Trata-se de um sistema de entrega de certificados e de chaves criptográficas, que torna possível toda espécie de transações eletrônicas que envolvam partes relativamente desconhecidas (por exemplo, transações financeiras, transações comerciais, etc.).

Uma PKI deverá garantir o suporte necessário para a confidencialidade, o controle de acesso, a integridade, a autenticação e não repúdio das informações trocadas pelas partes. Para tanto, são suas funções o gerenciamento da geração e a distribuição de pares de chaves públicas e privadas e a publicação de chaves públicas com as identificações de seus titulares (na forma de certificados) em diretórios abertos à consulta geral.

A atuação da PKI visa garantir, basicamente: um alto grau de confiança em relação à segurança das chaves privadas, o fato de determinada chave pública estar vinculada a uma determinada chave privada e a real identidade do titular de cada par de chaves assimétricas geradas. Além de tais garantias de cunho mais jurídico, as PKI também podem garantir e atuar em relação a outras questões importantes, referentes à tecnologia em si (como, por exemplo, assegurando a compatibilidade técnica dos meios utilizados para a obtenção da firma eletrônica adotada como padrão).

Geralmente, uma PKI, conforme MICCOLI (2003, p. 17), "é estabelecida pelo agrupamento hierárquico de várias Autoridades Certificadoras". Cada chave pública

e identificação de determinado usuário do sistema (pessoas físicas e jurídicas comuns) é posta em uma mensagem chamada de certificado. A Autoridade Certificadora responsável por esse usuário aporá sua firma digital sobre o certificado emitido, colocando-o em um diretório de certificados aberto à consulta pública (publicação do certificado). Dessa forma, qualquer pessoa poderá ter acesso à chave pública certificada, daquele usuário específico, e efetuar a autenticação dos documentos eletrônicos portadores de sua firma digital.

Observa-se que a própria Autoridade Certificadora deverá possuir um certificado, uma vez que ela está apondo uma firma digital sobre os certificados dos usuários vinculados a ela. Pode-se dizer, então, que deverá haver outra Autoridade Certificadora, hierarquicamente superior, responsável por gerenciar certificados e chaves das Autoridades Certificadoras do primeiro nível.

Numa cadeia, portanto, tem-se que a Autoridade Certificadora no topo da hierarquia deverá firmar digitalmente os certificados contendo as chaves públicas das Autoridades Certificadoras diretamente subordinadas a ela, e estas, por sua vez, firmarão digitalmente os Certificados das Autoridades Certificadoras abaixo delas e assim por diante, até chegar-se no nível das Autoridades Certificadoras que firmam, de acordo, e segundo MICCOLI (2003, p. 17), "digitalmente os certificados de chaves públicas dos usuários normais (pessoas físicas ou jurídicas)". Obviamente que, a depender da legislação específica adotada por cada país, a forma de organização e o número de níveis de uma PKI pode variar muito.

> O futuro legislador do comércio eletrônico deverá preocupar-se em enquadrar corretamente o sistema interno das *C. A.*, cuidando de estabelecer funções, requisitos e responsabilidades. Sobretudo no caso da *C. A.* será necessário ter o cuidado de coordenar o sistema com o resto da legislação estrangeira, porque é evidente que, sobre as autoridades certificadoras que garantem o serviço, deverão existir outras autoridades certificadoras superiores, seja em nível nacional, seja em nível supranacional, de modo que se possa garantir a vinculação, em base mundial, dos singulares sistema infraestruturais do comércio eletrônico (MICCOLI, 2003, p. 18).

Observe-se, que existe a tendência de criação de uma PKI em nível mundial, supranacional, destinada a garantir a necessária confiabilidade para as transações internacionais. A Autoridade Certificadora de topo nessa hierarquia seria, por exemplo, gerida por vários países, e encarregaria de garantir as PKIs existentes (provavelmente a partir da Autoridade Certificadora interna de mais alto nível) em

cada país que a ela se afiliasse. Pode-se imaginar, ainda, que os certificados emitidos para as transações internacionais possam ser padronizados e adequados a seu uso supranacional, possuindo um conjunto de informações diferente daquele contido nos certificados internos estabelecidos por cada país (em razão das próprias diferenças dos vários ordenamentos).

Nesse caso, poderia ser criada uma PKI completamente independente das estruturas internas de cada país, somente dedicada às relações internacionais, acarretando a necessidade, para o usuário comum, de possuir dois pares de chaves assimétricas com seus dois respectivos certificados: o primeiro, vinculado a uma PKI nacional e destinado a uso interno em seu país de origem e, o segundo, vinculado a uma PKI internacional e destinado a uso em transações fora do país.

Uma das atividades que poderiam ser reguladas e colocadas a cargo das Autoridades Certificadoras seria o arquivamento (para fins de publicidade) de documentos eletrônicos e, ainda, a faculdade de transformação de um documento eletrônico em um documento tradicional, sobre o papel, com toda a eficácia jurídica do documento eletrônico que o originou (ou seja, ter-se-ia, no caso, o documento eletrônico como um original e o respectivo documento impresso em papel como cópia certificada).

3.4. DOCUMENTO ELETRÔNICO COMO MEIO DE PROVA

Este tópico te como objetivo apresentar a análise da prova documental como conceito jurídico com enfoque no documento eletrônico como documento probatório; a falsidade documental; a negativa da autoria: a questão do ônus da prova; ilícito tributário e o comércio eletrônico e a regulamentação do comércio eletrônico.

3.4.1. Documento Eletrônico como Documento Probatório

Entre os doutrinadores nacionais, há quem não consiga enquadrar na noção clássica de documento o conceito de documento eletrônico. Conforme GICO JÚNIOR (2003, p. 11) "sendo o documento sempre uma coisa, e, na visão deles, não

sendo o documento eletrônico tangível, não seria possível dizer que este é espécie daquele na concepção clássico".

No entender de MARCACINI (2003, p.4), "um conceito atual de documento deveria privilegiar o pensamento ou o fato que se quer perpetuar e não a coisa em que estes se materializam". Para o autor, o documento eletrônico seria totalmente dissociado do meio em que foi originariamente armazenado, vez que assumiria forma de uma seqüência de *bits*, não sendo o documento eletrônico outra coisa que não a seqüência mesma, independentemente do meio em que foi gravado. Assim o arquivo eletrônico em que está este texto poderia ser transferido para outros meios, sejam disquetes, CDs, ou discos rígidos de outros computadores, mas o documento eletrônico continuaria o mesmo.

> Ao longo do tempo a doutrina tem definido o documento como algo material, uma *res*, uma representação exterior do fato que se quer provar e que sempre conhecemos a prova documental como a maior das provas, pois consistente da representação fática do acontecido. Na esteira desses pensamentos, ao ligarmos indelevelmente o fato jurídico à matéria como uma coisa tangível, teríamos dificuldades em conceituar o documento eletrônico, pois este é intangível e etéreo, e muito longe se encontra do conceito de coisa como matéria (BRASIL, 2003, p. 1).

Existe uma imensa dificuldade de se produzir qualquer tipo de prova a respeito dos comportamentos delituosos na rede vez que o meio em que eles se dão é meramente virtual e, portanto não material. Segundo GICO JÚNIOR (2003, p. 135), "a acepção de documento no ciberespaço refere-se, efetivamente, a algo muito mais fluido do que a acepção tradicional na teoria do processo".

Para MARCACINI (2003, p.4), "o documento eletrônico é uma seqüência de *bits* que, traduzida por meio de determinado programa de computador, seja representativa de um fato". Sendo perpetuidade (representatividade futura) uma característica do documento, com o desenvolvimento da técnica, na opinião do autor citado, é possível criar documentos eletrônicos com perpetuidade mas desconexos de algo tangível.

Em primeiro lugar, não entende-se que a noção clássica de documento se restrinja à coisa. Na realidade, vários juristas se preocuparam em distinguir documento, registro do fato - prova -, e suporte do documento, a coisa sobre a qual se sustenta – meio de prova. CHIOVENDA (1998, p. 186) define documento como

"representação material destinada a reproduzir determinada manifestação do pensamento", não exigiu ele que a representação fosse indissociável de seu suporte, tão somente exigiu-lhe materialidade, no sentido de perpetuidade, contrapondo-se à natural volatilidade da palavra oral.

Conforme MOACYR AMARAL SANTOS (1972, p. 41), "o documento é a coisa que serve para representar outra, ou seja, a coisa feita destinada a fixar de modo permanente, ou durável, reproduzindo-os, os fatos ou manifestações do pensamento". O autor argumenta que o documento é esta coisa que serve para representar outra, pensamento ou fato, e tem o caráter de perpetuidade, durabilidade, comum aos documentos. A idéia que norteia este e a maioria dos autores não é contrária, em ponto algum, ao entendimento do documento eletrônico como documento na acepção jurídica da palavra.

Na Itália, onde o princípio também é consolidado, não encontra-se na doutrina maiores resistências ao enquadramento do documento eletrônico nas definições clássicas, sendo incontroversa para a maioria a sua utilização como tal. Para Montesano citado por GICO JÚNIOR (2003, p. 12), "a força probatória dos documentos informáticos deveria ser reconduzida ao regime do artigo 2.712 do *Condice Civile* italiano, que trata das reproduções mecânicas". O artigo 383 do Código de Processo Civil tem clara inspiração nele.

> Na França o problema não se põe, como no Direito anglo-americano, em termos de receptibilidade ante as Cortes dos Tribunais, mas em termos de exigências legais pertinentes, de uma parte à conservação e, de outra parte, à conclusão das transações. Estes impedimentos são muito semelhantes aos que sustentam alguns doutrinadores pátrios (GICO JÚNIOR, 2003, p. 13).

Para o autor supra citado, o Código Civil francês, em seu artigo 1.341 continua a exigir documento autêntico ou documento particular assinado para atos jurídicos que excedam determinada soma ou valor determinado por decreto. Mas o artigo 1.347, com a nova redação de 1980, regula o chamado princípio de prova, definindo-o como todo ato de forma escrita que tenha sido emitido por aquele contra qual o pedido é formulado ou daquele que o representa e que torna verossímil o fato alegado. Há quem sustente que este diploma é essencial para o Direito Informático como base legal para a utilização de documentos eletrônicos, mas o ponto ainda parece controverso.

BRASIL (2003, p.21) argumenta que "o registro em suporte informático proveniente de escritos tradicionais e a transcrição dos impulsos magnéticos ou eletrônicos provenientes do computador constituem, incontestavelmente, cópias". Na opinião dos autores, esta discussão é antiga na França e muito se evoluiu nestes últimos anos, ainda mais com a diretiva da União Européia para padronização da legislação concernente ao comércio eletrônico, inspirada na Lei Modelo da UNCITRAL. Hoje, não há muita resistência por parte das autoridades francesas em atribuir ao documento eletrônico o seu devido valor probatório.

> Já no Direito anglo-americano, as principais barreiras eram as chamadas regras de exclusão de provas, a *Hearsay Rule* (Regra de Ouvir Dizer) e a *Best Evidence Rule* (Regra da Melhor Prova). Em virtude da *Hearsay Rule* um documento não pode ser feito valer em um Tribunal se o seu autor não está presente paraprestar testemunho sobre o conteúdo e para submeter-se ao exame de contradição (*cross examination).* A *Best Evidence Rule* reza que apenas os documentos originais podem ser utilizados em Tribunais para fins de prova, não se pode utilizar uma cópia. Os juristas anglofonos encontraram certas dificuldades em convencer o júri de que o *output* constante de uma banda, disquete ou outro meio de armazenamento qualquer era, de fato, um documento original (GICO JÚNIOR, 2003, p. 13, 14).

A *United Nations Commission on International Trade Law,* conhecida como UNCITRAL e parte integrante da ONU, fez a minuta de uma lei sobre as relações comerciais por meio da *internet.* Segundo GOIS JÚNIOR (2001, p. 136) "suporte de aconselhamento para que os diversos países possam seguir uma única diretriz". No projeto, a UNCITRAL sugere que as leis nacionais sejam aproveitadas ao máximo, com o uso das lei civis que dão validade e reconhecem a existência dos atos jurídicos, bem como a questão da sua prova.

O documento escrito, tal como se conhece por sua materialidade, garante a existência da vontade das partes e a sua inalterabilidade. Com um simples exame pericial, apura-se a veracidade de sua originalidade e a autenticidade de sua assinatura. A UNCITRAL estabelece que para que o documento eletrônico tenha o mesmo valor probatório dos documentos escritos é preciso que eles tragam o mesmo grau de segurança contido nestes, conforme GOIS JÚNIOR (2001, p. 136), "sendo que para que isto aconteça é necessário o uso de processo criptográfico de certificação".

> Vários países já adotaram o modelo da UNCITRAL, como os Estados Unidos, a Alemanha, A França, a Argentina, Colômbia e outros que estão ultimando as suas legislações. No Brasil os

> Projetos de Lei n. 1.483/1999 e 1.589/1999 dispõem sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital em moldes bem próximos daqueles recomendados pela ONU (GOIS JÚNIOR, 2001, p. 136).

De acordo com o autor acima citado, acessar um *link*, baixar informação de um servidor, carregar dados em um computador remoto são operações típicas do ambiente de rede que podem vir a configurar comportamento delituoso. Entretanto, não deixam nenhum sinal, marca, pista física que possam comprovar a sua realização. Esse é, efetivamente, um problema sério no campo da efetivação dos modelos legais pensados para regular o ciberespaço. Com o tempo vêm se aprimorando os métodos de coletar dados de acesso para se saber quem acessou, linkou, baixou dados ou carregou informação em um micro. Esse processo entretanto, não é automático nem natural como impressões digitais ou vestígios de sangue ou sêmen.

Com o uso de *bots,* ou seja, pequenos programas que agem como um vigia eletrônico da rede (*robot)*, no entender de GOIS JÚNIOR (2001, p. 137) "é possível se construir um banco de *log* onde fiquem armazenadas informações de acesso a um *site* ou serviço da rede". O autor argumenta que os *bots*, entretanto, têm que ser implementados por alguém, em geral pelos provedores, que, em face da atual política de não responsabilização, não têm nenhum interesse em fazê-lo.

> Com o uso de *Page Views* ou *click through*, por exemplo, é possível saber quantas pessoas acessaram um determinado *site*. Com um pouco mais de tecnologia se conseguiria, inclusive dados capazes de levar um rastreamento do acesso como, por exemplo, o *IP* do computador que acessou o servidor (GOIS JÚNIOR, 2001, p. 136).

O autor ressalta que existem a outras formas de análise de tráfego de *sites* como a contagem de visitas, *sessions*; visitantes, *visitors* e; organizações, *organizations*. Essas ferramentas, entretanto, altamente técnicas, chegaram primeiro ao mundo dos negócios do que ao mundo do direito e isso sempre é prenúncio de problemas jurídicos difíceis de serem resolvidos.

Assim, na esteira dos novos delitos surgidos com o advento da rede nasceu também em muitos juristas a preocupação de promoverem uma dinamização da justiça através da institucionalização de novos meios de produção de provas utilizando-se das facilidades do meio cibernético. Pode-se esperar para em breve

inovações no sistema jurídico de diversos países no sentido de regulamentar inovações como a audiência virtual que já começa a ser praticada inclusive no Brasil, mesmo em falta de lei regulamentadora a respeito.

GICO JÚNIOR (2003, p. 14), comenta que seja por uma ou outra regra, um documento eletrônico não podia valer perante uma autoridade judicial: "o computador, com efeito, não poderia submeter-se a um contraditório e, portanto, a doutrina e a jurisprudência consideravam os documentos eletrônicos sempre uma prova por ouvir dizer". Esta situação perdurou mais ou menos até o final da década de 70.

Ainda comenta que a solução foi ampliar a noção de indisponibilidade do original (exceção à regra de exclusão) para contemplar documentos eletrônicos. A jurisprudência aceitou com largueza esta exceção. Mais ainda quando o documento eletrônico era desfavorável à entidade criadora do mesmo, assimilando esta prova documental à prova documental desfavorável gerada pelos empregados autorizados do litigante.

Segundo GICO JÚNIOR (2003, p. 14), "na realidade, a aceitação dessas construções jurídicas foi tamanha que se criou um problema". O autor ressalta que foi preciso combater a aceitação cega pelos júris civis e criminais da credibilidade de todos os documentos eletrônicos. Vários trabalhos científicos e decisões judiciais chamaram a atenção para a necessária seleção, entre o material probatório informático, do material confiável, separando-o do lixo informático. As questões metodológicas da avaliação dos dados conservados em memória pelo computador assumiram uma grande importância, em especial no tocante ao controle da boa conservação dos dados e processos de autenticação da origem dos registros. Hoje, esta questão está superada, existindo inclusive legislação específica sobre autenticação de documento eletrônico em vários estados e o seu uso processual.

3.4.2. Sobre a Falsidade Documental

A falsidade documental, em relação ao documento tradicional, subdivide-se em falsidade ideológica e falsidade material. A questão da falsidade ideológica foge do escopo do presente trabalho, uma vez que não é passível de averiguação através

do documento em si (seja ele tradicional, seja eletrônico), já que ele se apresenta materialmente perfeito. A espécie de falsidade documental que poderia ser averiguada seria a chamada "falsidade material". Esta, por suas características, é que se sujeitaria a ser objeto de análise no âmbito específico dos documentos eletrônicos, dentro do modelo "Firma Digital / Autoridade Certificadora".

Contudo, o termo "falsidade material", em tal contexto, perde um pouco de seu sentido, pois, no caso dos documentos eletrônicos, tal falsidade não é passível de apuração mediante verificação do suporte material, como se daria em relação aos documentos tradicionais. Não é por outra razão que TAGLINO (2003, p. 6) pondera que" aceitando a tese de documento informático como dado informático, ou seja, como conteúdo de pensamento privado de materialidade, "não se poderia falar mais, para o falso informático, de falsidade material, de falsidade ideológica, de falso por supressão, mas de cancelamento e substituição dos dados, de emissão de um dado falso".

Realmente, ante tudo o que foi exposto acerca da capacidade de autocertificação apresentada pelo conteúdo de um documento eletrônico, ou seja da firme "imutabilidade lógica" por ele apresentada, pode-se dizer que sua integridade é garantida em grau muito superior à de um documento tradicional sobre papel. Não existe possibilidade de alterar-se o conteúdo de um documento eletrônico portador de firma digital sem, com isso, invalidar-se essa firma digital e, consequentemente, sem que a existência de tal alteração se torne conhecida e facilmente comprovável.

Não existe possibilidade, também, de existir uma chave privada qualquer que seja capaz de produzir uma firma digital que possa corretamente ser decifrada com uso de uma chave pública que com a citada chave privada não faça par. Não existe, em suma, a possibilidade de existência de duas chaves privadas (uma delas, seria a utilizada pelo suposto falsário) que produzam um mesmo efeito, possibilitando que uma única chave pública de uma pessoa consiga decifrar corretamente.

Assim, pode-se dizer que a "falsidade material", no âmbito dos documentos eletrônicos, até poderia existir, se por tal se entendesse, estritamente, uma adulteração que possa ser feita em seu conteúdo. Todavia, essa adulteração não assume maior relevância, pois, de imediato, ela pode ser detectada e comprovada. Isso significa que ela não tem possibilidade de atingir seu fim (fazer crer em algo

falso). Pode-se dizer, portanto, que a "falsidade material", no âmbito dos documentos eletrônicos, é um incidente de fácil comprovação, não assumindo, nem de longe, a relevância que apresenta em relação aos documentos tradicionais, caso em que há dificuldades em sua comprovação (já que, para tal, comumente, seria necessária a feitura de complicadas perícias técnicas).

MARCACINI acerca da questão da falsidade documental, em relação aos documentos eletrônicos, afirma:

> [...] é possível afirmar que, quanto a um documento assinado eletronicamente pelo uso de criptografia assimétrica, a argüição de falsidade só poderá ser baseada em *'falsidade de assinatura* '. Isto porque a adulteração do conteúdo do documento é inviável, vez que faz perder o vínculo entre este e a assinatura. Dentro deste prisma, é de se dizer que o documento eletrônico assim assinado é dotado de um maior grau de confiabilidade que o próprio documento tradicional. O próprio *software* de criptografia, ao conferir a assinatura, acusa que o documento adulterado não corresponde a ela (MARCACINI, 2003, p. 16).

Já o documento cartáceo necessita de um exame pericial para provar uma eventual alteração; e, com o evoluir da técnica, certamente surgem meios mais e mais poderosos para alterar documentos físicos.

> Por *'falsificação da assinatura digital'* quero dizer a criação de um par de chaves falso, atribuído ao suposto signatário. A verdadeira assinatura digital, legitimamente gerada pelo seu titular, não tem como ser falseada. No fundo, inexiste falsidade a ser apurada no próprio documento eletrônico; o problema em análise se resume exclusivamente na verificação da autenticidade da chave pública. Sabendo ser autêntica a chave pública, o próprio programa de computador permitirá conferir a autenticidade e integridade do documento eletrônico (MARCACINI, 2003, p. 16).

O único modo de produzir documentos originais é através do uso de uma 'chave secreta' que somente o firmatário conhece, e que não deve ser por essa razão nunca revelada; desse modo, a única maneira para falsificar um documento é a aquisição, mediante furto ou através do erro, da chave secreta.

RAGOZZO & GIAQUINTO se posicionam entre aqueles que entendem que só existe um modo de produção de documentos eletrônicos falsos:

> Sabemos que, se verificamos positivamente um documento com a chave pública de Tício, ele deve ter sido, necessariamente, firmado usando a chave secreta de Tício, que se presume seja conhecida somente por Tício. O único modo para poder produzir documentos falsos seria o de subtrair de Tício a sua chave secreta. No caso de perda ou furto da chave secreta, Tício comunica imediatamente o fato à autoridade (no caso, o notário) que administra as chaves públicas, e daquela data em diante a chave pública cessará de possuir validade, continuando

> todavia a fazer fé para os documentos redigidos *seguramente* em data anterior (RAGOZZO & GIAQUINTO, 1997, p. 19).

CAMMARATA (2003, p. 11) faz raciocínio sobre a mudança de enfoque em relação à falsidade, decorrente da existência dos documentos eletrônicos: "a 'perícia caligráfica' e outros procedimentos análogos não terão mais motivos para existir, mas deverão ser constituídos outros procedimentos", como a verificação do momento de publicação ou de revogação da firma digital, das eventuais manobras escusas por parte das autoridades certificadoras, da possibilidade de conhecimento da chave privada de parte de um sujeito diverso do titular e, sobretudo, do eventual engano sobre a identidade do interessado no momento da certificação da firma.

Este é o exemplo talvez mais interessante do salto cultural advindo da introdução dos documentos informáticos: onde hoje se procura um crime de falso pela aposição de uma firma falsificada, amanhã se deverá indagar sobre uma possível substituição de pessoa, no momento da certificação da firma. Os efeitos podem ser os mesmos, mas o crime é outro. A impossibilidade de distinção entre o *bit* verdadeiro e o *bit* falso, a bem da verdade, não existe, porque o documento que leva uma firma digital ou é verdadeiro, ou não é um documento. De acordo com VOLPI (2001, p. 37), "os algoritmos de chave assimétrica dão uma certeza próxima absoluta da autenticidade das informações, não podendo existir documentos verdadeiros com uma firma digital falsa, ou vice-versa".

Pode-se dizer, consequentemente, que não existe possibilidade de um documento eletrônico portador de firma eletrônica apresentar uma "falsidade material", de forma similar àquela que é concebida para os documentos tradicionais. Isso, não só porque tais documentos eletrônicos não se vinculam aos seus suportes materiais, mas, também, pelo fato de possuírem integridade auto-certificável. Assim, tem-se que, ou o documento eletrônico possui o conteúdo que nele foi posto e aceito por aquele que sobre ele calculou sua firma digital, ou não se tratará de um documento eletrônico portador de firma digital, uma vez que, tendo havido perda de integridade, há também perda de autenticidade (a firma digital fica invalidada). O único modo possível de haver falsidade em um documento eletrônico seria, portanto, o uso indevido de uma chave privada, por uma pessoa que não fosse o seu legítimo titular.

3.4.3. Sobre a Negativa da Autoria: a Questão do Ônus da Prova

A negação de uma firma digital, por ser uma exceção que pode ser objeto de verificação imediata, pode ser prontamente rejeitada em juízo, se comprovadamente infundada. A comprovação se dará pela forma já explicada, ou seja, através da decifragem do documento eletrônico portador de firma digital, com uso da chave pública certificada daquele que nega a sua paternidade. O próprio juiz, munido somente do *software* adequado, poderá executar o procedimento, de maneira simples e rápida. Resultando positiva a autenticação do documento, à luz do liame propiciado pelo modelo "Firma Digital / Autoridade Certificadora", não há facilidade para sustentar a negativa. Trata-se do não repúdio sendo implementado de forma eficiente, sem demandar nenhuma perícia técnica, como seria imprescindível caso a negação tivesse se dado em relação a uma assinatura tradicional.

ZAGAMI (2003, p. 28) aponta uma única negação aceitável, em relação à firma digital, indicando sobre quem pesaria o ônus da prova: "uma negação aceitável poderia somente consistir na exceção que a firma digital tenha sido aplicada empregando uma chave privada por parte de quem não era seu legítimo titular (por exemplo, porque foi furtada ou perdida)". Mas, neste caso, o ônus de provar a invalidade da firma toca à pessoa que apareça como subscritor do conteúdo do certificado. É do fato de se estabelecer um ônus de custódia da chave privada, indispensável para o correto funcionamento do sistema em sua inteireza, que se verifica, neste caso, uma inversão do ônus da prova.

Em conclusão, na escritura privada tradicional, no caso de negativa, o ônus de acionamento do procedimento de verificação toca à parte que tenha produzido o documento; ao contrário, em uma escritura privada com firma digital negada, o ônus de demonstrar a falsidade da firma – no sentido supra indicado – toca àquele que resulta ser o subscritor. Aquilo que se desconhece é, em substância, a exclusividade do uso do aparato técnico – que é a chave privada – que vem presumido, salvo prova em contrário.

Observa-se que as possibilidades válidas, de negativa de autoria (decorrentes de furto ou perda), para poderem sustentar-se, têm estreita relação com a questão da data dos documentos eletrônicos. Isso porque, assim que percebido o furto ou a

perda, seria o caso de existir uma obrigação do titular em efetivar a revogação do seu certificado (com ele, revogadas estariam suas chaves pública e privada), sob pena de sua responsabilização pelos atos indevidamente praticados em seu nome. A datação, nesses casos, é importante porque, a partir do momento (data e, inclusive, hora) da revogação do certificado, os documentos com a firma digital revogada não permanecerão válidos, podendo ter sua autoria eficazmente negada pelo titular das chaves revogadas. Porém, no caso dos documentos eletrônicos portadores de firma digital do autor, anteriores à revogação, tem-se que permaneceriam integralmente válidos.

Conforme MARCACINI (2003, p. 9), "diante da argüição de apropriação e uso indevido da chave privada verdadeira, o ônus da prova competirá a quem alegar este fato". Quando a segurança de uma chave privada for posta em dúvida, é possível que ela seja revogada. Alguns problemas, entretanto, podem ser vistos aqui: por primeiro, a necessidade de publicidade da revogação; em segundo lugar, a impossibilidade de se atribuir, por si só, certeza às datas da revogação ou da assinatura indevidamente efetuada pelo criminoso com o uso da chave privada apropriada. Daí, talvez o problema da datação de documentos eletrônicos deva ser observado com o máximo de cautela e, no mais das vezes, será conveniente estabelecer meios seguros de provar a data do documento eletronicamente assinado.

3.4.4. Ilícito Tributário e o Comércio Eletrônico

O desenvolvimento do comércio eletrônico impõe desafios à tributação, tanto quanto na gestão das administrações tributárias públicas como das empresas.

Primeiramente, cabe-nos ressaltar o que é um 'ilícito tributário'. Na acepção da palavra "ilícito" , conforme o Dicionário prático Michaelis, significa o "que não é lícito, contrário às leis ou à moral". No universo jurídico, os comportamentos podem ser classificados como lícitos ou ilícitos. Os primeiros são aqueles que estão de acordo, e os últimos, aqueles contrários à ordem jurídica, ao direito objetivo.

O ilícito tributário configura um comportamento que implica inobservância de norma tributária, que implica em inadimplemento de obrigação tributária, seja ela

principal ou acessória. A obrigação tributária principal ou acessória é assim definida pelo CTN (Código Tributário Nacional) em seu artigo 113:

> Art. 113. A obrigação tributária é principal ou acessória.
>
> § 1 A obrigação principal surge com a ocorrência do fato gerador, tem por objeto o pagamento de tributo ou penalidade pecuniária e extingue-se juntamente com o crédito dela decorrente.
>
> § 2º A obrigação acessória decorre da legislação tributária e tem por objeto as prestações, positivas ou negativas, nela previstas no interesse da arrecadação ou da fiscalização dos tributos.
>
> § 3º a obrigação acessória, pelo simples fato da sua inobservância, converte-se em obrigação principal relativamente a penalidade pecuniária (OLIVEIRA, 1994, p. 48-49).

Dessa forma, caracteriza-se como ilícito tributário, a inobservância das normas tributárias, sejam elas federais, estaduais ou municipais tanto no aspecto da obrigação principal quanto no da obrigação acessória, ou seja, a falta de pagamento de tributos ou penalidade pecuniária e a emissão dos documentos de circulação de mercadorias e serviços e de controle de interesse da arrecadação e fiscalização dos tributos.

O comércio eletrônico via internet envolve a venda de bens e mercadorias tangíveis (aparelhos eletrônicos, eletrodomésticos, microcomputadores, brinquedos, entre outros) e de bens intangíveis (softwares, músicas, jogos eletrônicos, etc...), onde a operação começa, se desenvolve e termina nos meios eletrônicos, podendo as transações serem realizadas por e-mail, contratos eletrônicos, e o pagamento ser efetuado via cartão de crédito ou débito bancário.

O que difere uma transação de um bem pelo meio eletrônico e a venda do mesmo bem pela via tradicional, senão o meio empregado para a compra e a venda. O fato imponível dos impostos, principalmente o ICMS (Imposto sobre operações relativas à circulação de mercadorias e sobre a prestações de serviços de transporte interestadual e intermunicipal e de comunicação), concretiza-se da mesma forma, e, em ambos os casos, surtirá a necessidade do respectivo cupom fiscal ou da nota fiscal, para que se promova, posteriormente, o recolhimento dos impostos devidos.

No caso de venda por meio do e-commerce de bens tangíveis e entrega física, os tributos sobre a circulação de mercadorias e outros aplicáveis incidirão da

mesma forma que no comércio tradicional, onde os produtos são entregues por uma empresa normal, não virtual.

Mesmo havendo a circulação física do produto, o fato de a transação ser efetuada via internet, dificulta o controle da documentação fiscal que deve acompanhar a mercadoria, visto que muitos dos produtos vendidos são geralmente, remetidos diretamente ao domicílio do consumidor por meio da rede de correios, ou por transportadoras.

Todavia, a grande dificuldade para as administrações tributárias, se dá por conta da tributação dos produtos e serviços chamados intangíveis, principalmente os que se configuram como prestação de serviços (compra de programas de computador via rede ou execução de programas, músicas, filmes, disponibilização de jogos virtuais, etc.) onde o produto adquirido é entregue via internet, (baixa de software no próprio computador) inexistindo, assim, a emissão de cupom ou nota fiscal para documentar a incidência do imposto devido, configurando o ilícito tributário, ou seja, a venda de mercadoria ou serviço sem a emissão da correspondente documentação fiscal e, consequentemente, sem o recolhimento dos tributos devidos.

Em ambos os casos, o documento eletrônico, seja ele e-mail, contratos, transferências de fundos, recibo de pagamento através do cartão de crédito serão emitidos via internet para documentar a transação entre o vendedor e o comprador e ficarão armazenados por certo tempo nos sistemas dos mesmos. Caso haja ilícito tributário numa dessas transações, tanto de mercadorias tangíveis quanto não tangíveis, como o tributo poderá ser exigido pelas autoridades fiscais tributárias diante de tal situação? GICO JUNIOR (2003, p.20) comenta que, em uma análise de documentos apreendidos por autoridades fiscais e policiais durante a auditoria de uma empresa, onde foram apreendidos documentos e computadores, ao analisar os documentos e arquivos eletrônicos existentes nos computadores, constata que havia desvio no fluxo de caixa, o chamado caixa dois, e procedem a autuação fiscal tributária na empresa auditada: questiona-se "algum jurista é capaz de afirmar que não é possível autuar a empresa com base apenas nos registros encontrados em seu computador?". Outro exemplo citado pelo autor, sobre o documento eletrônico

como prova de ilícito, está relacionado à pornografia infantil via internet, quando as autoridades policiais e Ministério Público descobrem através de rastreamento de e-mail e de informações providas pelo provedor de acesso, o endereço do suspeito e invadem a sua residência ou escritório, encontrando somente os registros do computador que é apreendido: as fotos, endereços de seus clientes, contabilidade da atividade, e-mail enviados e recebidos, etc.. "Alguém, em sã consciência dirá que esse sujeito, preso em flagrante, não será julgado por ausência de provas? É possível afirmar em juízo que ele é o autor ou portador ilegal de tais documentos? É claro que não" (GICO JÚNIOR, 2003, p. 20).

Na prática os auditores fiscais, sejam federais, estaduais, se utilizam de documentos eletrônicos, cópias de arquivos eletrônicos, como planilhas de custos, relatórios de compras e vendas, depósitos bancários efetuados via internet, para fazerem prova contra quem os emitiu, extraindo deles, documentos, informações e dados de indícios de ilícitos fiscal tributário. O que falta na realidade ou grande obstáculo da plena utilização dos documentos eletrônicos como meio de prova, ainda é a falta de regulamentação dos mesmos. Esse é o tema abordado no próximo tópico.

3.4.5. Regulamentação do Documento Eletrônico

Apesar do comércio eletrônico já negociar expressivos valores de forma virtual, ainda não existe uma definição legal do documento eletrônico no Brasil e da mesma forma não há uma legislação específica que dê proteção aos negócios eletrônicos.

Os Projetos de Lei existentes buscam regulamentar a Internet, equiparando a assinatura digital àquela convencionalmente posta em um suporte físico, com o propósito de que as relações eletrônicas possam ter a mesma eficácia das tradicionais.

Em respeito a todas essas funções que o documento em papel proporciona, a Lei modelo da UNCITRAL estabelece que os registros eletrônicos, para que recebam o mesmo nível de reconhecimento legal, devem satisfazer, no mínimo, o

mesmo grau de segurança que os documentos em papel oferecem, o que deve ser alcançado por de uma série de recursos técnicos. Em suma, a Lei modelo estabelece uma série de requisitos para que um documento eletrônico alcance uma função equivalente ao documento escrito, assinado e original.

Em se tratando de documento eletrônico, a ordem jurídica nacional não se ajustou à nova realidade existente em no Brasil, visto que até o presente momento, o assunto em questão não recebeu tratamento jurídico.

Em agosto de 2001 foi expedida a Medida Provisória 2.200-2 que institui a infra-estrutura de Chaves Públicas Brasileira – ICP – Brasil, e cria o Comitê Gestor de Políticas como órgão apto a fornecer os certificados eletrônicos, que irão garantir a segurança e demais aspectos já delineados dos documentos eletrônicos.

Para suprir a deficiência da legislação já existente e ajustar o Brasil à nova conjuntura mundial, vem sendo elaborado uma grande variedade de Projetos de Lei no país, todos com o propósito de regulamentar a validade do documento eletrônico (através da certificação digital e da criptografia assimétrica), mas, sobretudo, o próprio comércio eletrônico, os crimes a ele inerentes e os efeitos jurídicos decorrentes das relações jurídicas que lhes são afetas.

Para isso está em tramitação no Congresso Nacional os projetos de lei 1483/99, apensado ao PL 1589/1999 que dispõe sobre a validade jurídica e o valor probante do documento eletrônico e da assinatura digital, regula a certificação digital e institui normas para as transações do comércio eletrônico. Ainda há os projetos 4906/2001 de autoria do Senado federal que trata normas para as transações de comércio eletrônico, a validade jurídica de documentos eletrônicos, assinatura e certificação digitais, o projeto de lei apresentado pelo Poder Executivo de número 7.316/02 que define a assinatura eletrônica avançada, a chave de criação e de verificação de assinatura e o certificado digital qualificado e ainda estabelece requisitos para que a Autoridade Certificadora Raiz da infra-estrutura de Chaves públicas Brasileira realize o credenciamento do prestador de serviço de certificação, e outro que merece destaque o Projeto de Lei da Casa Civil.

De todos as propostas anteriores, merecem destaque o Projeto de Lei de autoria da Casa Civil e o Projeto de Lei nº 1.589/99. Para comentar o primeiro deles, recorre-se às anotações de Aldemário Castro. Em seu artigo Validade jurídica de

documentos eletrônicos: considerações sobre o projeto de lei apresentado pelo governo federal, apresenta os seus defeitos e aponta as suas virtudes, que podem ser assim resumidas:

> a) limita-se ao setor público; b) não contempla a produção e a circulação de documentos particulares, mas tão somente o seu arquivamento por meio magnético ou similar; c) adota a diretriz de não consagrar determinada tecnologia por edição de norma de direito; d) comete um erro inaceitável na definição da abrangência de seus efeitos; e) deixa de regular inúmeros aspectos cruciais relacionados com os documentos eletrônicos; e f) afasta a validade jurídica, hoje presente, dos documentos eletrônicos quando não asseguradas, por meio hábil, a autenticidade e a integridade (CASTRO, 2001. p. 6)

O Projeto de Lei nº 1.589/99 teve por autor o Deputado Luciano Pizzato e origem no anteprojeto de lei da OAB para o comércio eletrônico, que dispunha sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital. Traz apensado o Substitutivo ao Projeto de Lei nº 1.483, de 1999, que teve por autor o Deputado Dr. Hélio, e por relator o Deputado Júlio Semeghini. Para comentá-lo, recorre-se a Itamar Arruda Júnior. Em seu artigo Considerações ao PL n. 1589/99 esclarece que o documento:

> [...] é baseado no modelo da UNCITRAL e na diretriz da União Européia, dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital. No tocante a validade jurídica do documento eletrônico, as disposições daquele instituto são expressas ao considerar sua originalidade, sempre que for assinado pelo autor, utilizando-se da assinatura digital e do sistema de criptografia assimétrica, havendo, nestes casos, a presunção de veracidade do conteúdo do documento, em relação ao autor (ARRUDA JÚNIOR 2001, p. 6)

Comenta ainda o autor acima que:

> Entretanto, não se trata de presunção absoluta, sendo mister a observância de determinados requisitos, também elencados no anteprojeto, tais como; de que seja a assinatura digital única e exclusiva para o documento que foi firmado, seja possível a identificação de sua validade, que o acesso a assinatura eletrônica seja exclusivo do signatário, que esteja vinculada a totalidade do texto do documento, e que não tenha sido gerada após o prazo para a sua expiração, que segundo o instituto, será de 2 (dois) anos, na ausência de sua estipulação, quando, então, caberá a parte a quem a assinatura beneficiar comprovar que foi a mesma gerada em período anterior a expiração ou a revogação (ARRUDA JÚNIOR 2001, p. 6)

Com efeito o legislador brasileiro ainda carece de entendimento e afinamento com a doutrina nacional e tem trazido soluções do direito alienígena que não

satisfaçam à realidade brasileira. O que foi realizado até o presente momento carece de adequação e o setor necessita de regulamentação urgente, pois as propostas apresentadas ao Poder Legislativo demonstram incompletas.

4. CONSIDERAÇÕES FINAIS

Durante toda a exposição precedente, foram manifestadas não só as razões e pensamentos dos estudiosos mas, também, as adotadas pelo presente trabalho. Sendo assim, em termos de considerações finais, resta apenas registrar, em forma de retrospectiva, os aspectos mais relevantes identificados ao longo de toda a pesquisa efetuada:

A "Sociedade da Informação" veio para substituir a "Sociedade Industrial", de forma mais eficiente, possibilitando uma liberação do ser humano das tarefas mais repetitivas e burocráticas, abrindo espaço para que ele possa dedicar-se a tarefas mais criativas. As máquinas da Revolução Industrial multiplicaram a força e a capacidade de produção física do homem. As tecnologias da informação destinam-se a ampliar a sua inteligência e capacidade intelectual de produzir. Nesse novo tempo, deter informação é deter poder, por conseguinte, o tratamento adequado de grandes volumes de dados e informações adquire fundamental importância. A informação moderna não pode ser estática, tem que ser dinâmica, voltada para a ampla circulação. As tecnologias da informação se baseiam, sobretudo, no uso intensivo da informática e da telemática. Conhecê-las e saber como usá-las, portanto, passou a ser habilidade indispensável. O seu uso cotidiano é uma necessidade, e deve ser incentivado.

A grande rede, a *Internet*, é fenômeno de múltiplas facetas. Trata-se de ferramenta que se tornará, a cada dia, mais indispensável. Suas possibilidades são imensas, sendo o uso que dela se faz hoje, tão-somente, uma pequena parcela da potencialidade total que esse meio de integração mundial pode oferecer. O comércio eletrônico é um dos novos campos abertos pela popularização da Internet. Trata-se de tema que vem despertando grande interesse de estudiosos e governantes. Seu impacto sobre a economia mundial pode assumir proporções de difícil mensuração. Através dele, o mundo pode tornar-se um imenso e único mercado consumidor, amplamente acessível, de forma muito racional e a custos muito baixos. Não é sem razão, pois, que o comércio eletrônico tem sido o grande motor dos estudos relativos à viabilização dos documentos eletrônicos com validade jurídica (por conseqüência,

também das firmas eletrônicas). Essa nova forma de documentação é vista como o meio apto a possibilitar a celebração de transações seguras e devidamente tuteladas pelo Direito.

Um "documento", de forma genérica, é algo que tem por função primordial o registro confiável e durável de um fato. Um documento é dito jurídico quando registra fatos que tenham repercussão e relevância no mundo do direito; de outra forma, será considerado um documento histórico. Sua finalidade precípua é fazer conhecer o seu conteúdo, ao longo do tempo, a pessoas diversas. A sua materialidade é, em relação à sua finalidade maior, apenas um aspecto acessório. No âmbito da pesquisa realizada, constatou-se ser fundamental a diferenciação entre "documento" (elemento espiritual, conteúdo) e "forma de documentar" (elementos materiais, como o suporte e a escrita).

Para o Direito, a função maior de um documento é a de servir como elemento probatório. Nesse sentido, um documento jurídico deve ser confiável e deve poder ter essa confiabilidade aferida. Na falta disso, restará comprometida a sua eficácia probatória. A prova documental possui invulgar força de convencimento, disso derivando o extremo cuidado dos doutrinadores, legisladores e operadores jurídicos, até aqui, com os aspectos relativos à materialidade dos documentos em geral. Sempre foi através dela (do suporte material, da assinatura manuscrita, etc.) que a confiabilidade de uma prova encontrava meios de ser aferida. Aspecto que bem comprova a dependência que o documento (conteúdo) apresenta em relação ao suporte material – e à própria forma de documentar –, encontra-se na distinção que o Direito faz entre um documento dito "original" e um documento dito "cópia". O segundo, se produzido sem os devidos cuidados, perde toda ou grande parte de sua validade jurídica.

A avaliação da eficácia da prova documental (no caso dos documentos tradicionais), feita com base no suporte material, visa o suprimento de três requisitos essenciais: integridade, autenticidade e tempestividade. O primeiro se refere à inteireza de conteúdo do documento, ao grau de fidelidade que o mesmo apresenta em relação ao que o autor quis nele registrar. O segundo se refere à confirmação de que o documento tenha sido produzido por uma determinada pessoa e, somente dela, possa ter sido proveniente (aspectos relativos à imputação subjetiva e à

garantia do não repúdio). O terceiro, por fim, se refere à verificação de que o documento seja contemporâneo dos fatos que registra, não tendo sido obra engendrada, de forma ardilosa e fraudulenta, posteriormente aos mesmos.

Uma verificação dos dispositivos legais reguladores da matéria atinente à prova documental, constantes do Código de Processo Civil, confirma o acolhimento prático dos requisitos essenciais evidenciados pela doutrina.

Para que o Direito possa conviver com documentos eletrônicos jurídicos, é necessário entender-se e aceitar-se a idéia da "desmaterialização" do documento, trazendo-se o foco para o seu conteúdo e deixando-se o suporte num plano secundário. Torne-se a afirmar: o que importa é a obtenção de um registro eficiente e confiável de um fato e não a forma como isso se dá, na prática.

Não se deve confundir o documento eletrônico abordado em seu aspecto meramente operacional com o documento eletrônico abordado em seu aspecto jurídico, através do qual se procura revesti-lo de garantias capazes de dotá-lo de plena eficácia probatória.

Os requisitos essenciais a serem supridos para a obtenção da validade jurídica dos documentos eletrônicos são, basicamente, os mesmos verificados em relação aos documentos tradicionais (ou seja, integridade, autenticidade e tempestividade). Assim, pode-se afirmar que boa parte do conhecimento genérico acumulado, em relação aos documentos tradicionais e sua validade jurídica, pode ser aproveitado quando do idêntico acolhimento dos documentos eletrônicos. As formas de suprimento dos requisitos mencionados, contudo, são completamente diferentes. No caso dos documentos tradicionais, os requisitos essenciais são aferidos com base no suporte material, sendo que autenticidade possui, na assinatura manuscrita seu elemento de aferição mais importante. No caso dos documentos eletrônicos jurídicos, a aferição da integridade, da autenticidade e da própria tempestividade se baseiam em firmas eletrônicas. No caso prático do modelo "Firma Digital / Autoridade Certificadora", a base está nas firmas digitais do autor, das Autoridades Certificadoras e das autoridades dos serviços de estampagem de tempo. O modelo "Firma Digital / Autoridade Certificadora" é, atualmente, o modelo prático conhecido para implementação dos documentos eletrônicos jurídicos, sendo reputado como seguro, tanto por estudiosos quanto por legisladores. Sua

adequação e confiabilidade estão estreitamente vinculadas ao uso da criptografia assimétrica .

Muitos são os termos propostos e usados para referenciar o produto dessa nova forma de documentação (seja por estudiosos, seja por legisladores), dentre os quais pode-se citar "documento eletrônico", "documento informático" e "documento digital". No âmbito da presente pesquisa, conforme já se justificou, foi adotado o termo verificado como sendo de uso mais corrente ("documento eletrônico"), apesar de reconhecer-se a propriedade do termo "documento digital". Existem duas formas de abordar-se, conceitualmente, os documentos eletrônicos e os demais elementos que o conformam (firma eletrônica, por exemplo). A primeira, procura ser tecnologicamente neutra, na qual se busca frisar os requisitos essenciais a serem supridos sem, contudo, mencionar-se os meios concretos de tal suprimento. A segunda, é tecnologicamente vinculada ao modelo "Firma Digital / Autoridade Certificadora" (baseado na criptografia assimétrica), que conceitua com base nos meios concretos disponíveis e aceitos como eficazes para o suprimento dos requisitos exigíveis. Acredita-se que a primeira forma se mostra mais adequada ao texto de uma lei genérica, destinada a acolher os documentos eletrônicos jurídicos no ordenamento.

A segunda forma, por sua vez, seria mais apropriada para o texto das subseqüentes regulamentações dessa lei (decretos, por exemplo), destinadas a reger as aplicações e situações de ordem mais prática. Acredita-se que, dessa forma, o resultado seria uma lei (norma genérica) mais durável, por ser menos afetada pelas constantes inovações tecnológicas. As regulamentações e decretos, por sua vez, pelo seu conteúdo menos neutro, é que deveriam cuidar sofrer as adaptações necessárias ao longo do tempo.

O surgimento, na segunda metade da década de 70, da técnica de criptografia assimétrica foi um marco na história da informação digital. É através dela que, hoje, pleiteia-se a concessão do atributo "jurídico" aos "documentos eletrônicos", sempre tidos como inseguros e não confiáveis. Com o uso da criptografia assimétrica pode-se pensar em uma forma de "assinar" tais documentos (mediante aposição de uma firma eletrônica), dotando-os de firme garantia quanto à sua integridade, autenticidade e tempestividade. A firma eletrônica não deve ser

confundida com assinatura digitalizada (que é uma mera imagem digital de uma assinatura manuscrita), e nem com a firma digital (que é uma espécie do gênero firma eletrônica, vinculada à técnica específica da criptografia assimétrica). A firma eletrônica visa ser, tanto quanto possível, técnica e tecnologicamente neutra, devendo preocupar-se em expressar uma finalidade ideal e teórica. A firma digital, por sua vez, é uma forma de implementação prática de uma espécie do gênero firma eletrônica. Não se deve, ainda, confundir a função da firma eletrônica com a função das senhas (do tipo *PIN, password* ou *passphrase*) ou das firmas biométricas. A primeira visa uma garantia de autenticidade enquanto que as últimas servem, apenas, como forma de verificação de legitimidade (ou seja, uma espécie de autorização para executar uma determinada operação, tarefa ou ato).

Observe-se que uma transposição, pura e simples, das características da assinatura tradicional para a firma eletrônica resultaria sem sentido (não há autografia, nem legibilidade, muito menos sentido em se exigir aposição ao final do documento). Mediante o uso de uma firma eletrônica, o conteúdo do documento eletrônico fica auto-certificável. Isso significa que a verificação da autenticidade, integridade e tempestividade é feita com total independência em relação ao suporte material utilizado (no caso, alguma das espécies de suportes informáticos). Quando há duplicação de conteúdo, tudo o que é necessário para efetuar-se a autenticação do documento eletrônico também será duplicado. Por essa razão, também, é que a distinção entre "original" e "cópia" perde o sentido em relação aos documentos eletrônicos. Observe-se que essa auto-certificação é fácil de ser efetuada, é segura e não depende de quaisquer perícias técnicas (o próprio magistrado, por exemplo, poderia executar os procedimentos necessários).

Em relação aos documentos tradicionais, existem muitos problemas relativos à falsidade (a pagamentos, inserções indevidas, alterações de conteúdo, falsificação de assinaturas, etc.). Em relação aos documentos eletrônicos jurídicos, contudo, somente há um eventual problema do gênero: a falta de exclusividade do uso do meio técnico, ou seja, o uso indevido do meio capaz de produzir uma firma eletrônica por outra pessoa, que não o legítimo titular. Nesse sentido, somente a perda ou furto do segredo de aposição da firma eletrônica é que poderia, validamente, sustentar uma tentativa de repúdio em relação a um documento eletrônico jurídico

positivamente autenticado. Nesse caso, contudo, em função da obrigação de custódia de tal segredo, o ônus da prova do fato alegado seria do suposto autor do documento cuja firma eletrônica esteja sendo contestada, e não da outra parte, que o produziu em juízo. Pode-se dizer que não existe possibilidade de falsificação material, em relação ao conteúdo de um documento eletrônico jurídico. Isso porque a firma eletrônica vincula-se de tal forma ao conteúdo do documento eletrônico, que a menor alteração deste implica invalidação daquela (ou seja, o documento se torna apócrifo). Pela mesma razão, não existe possibilidade de preenchimento abusivo de um documento eletrônico firmado eletronicamente em branco. Pode-se dizer, portanto, que a garantia de integridade de um documento eletrônico jurídico é bem maior do que a de um documento tradicional.

A tutela e o acolhimento da nova forma de documentação que se apresenta, tornando-a segura e confiável, é uma necessidade cada vez mais premente. Além disso, não se pode esquecer que os documentos eletrônicos estão intimamente ligados à tecnologia (*bits*, *bytes*, suportes informáticos, computadores, telemática) e à técnica (criptografia). O conhecimento de tais novidades é fundamental para uma abordagem jurídica do tema ora em estudo. Aspectos técnicos, tecnológicos e jurídicos caminham de mãos dadas, vislumbrando-se, nessa interdisciplinaridade, o aparecimento de um "Direito Tecnológico".

Devido ao fato do documento eletrônico ser transmissível por natureza (essa é, inclusive, uma de suas maiores vantagens), ele deverá poder, se for o caso, circular por vários países, mantendo incólumes as suas propriedades jurídicas. A falta de uniformidade normativa, configurar-se-ia em um grande empecilho à circulação e difusão de uso dos documentos eletrônicos jurídicos (imagine-se o que isso significaria, em termos de entrave, por exemplo, para o desenvolvimento do comércio eletrônico).

A questão da segurança dos ambientes computacionais também assume grande relevância, no âmbito do tema ora pesquisado. Um dos pilares da validade jurídica dos documentos eletrônicos (no que se refere à questão da autenticidade), se encontra na "exclusividade de uso do meio técnico", exigida para a geração de uma firma eletrônica. Assim, como uma assinatura tradicional manuscrita, a firma eletrônica somente deve poder ser aposta, sobre um determinado documento, por

seu titular. O uso de documentos eletrônicos em ambientes computacionais inseguros – por exemplo, um computador infectado por um vírus "Cavalo de Tróia" com *key logging* ativado (ou seja, monitorando o que é teclado pelo usuário) –, comprometeria a exclusividade mencionada, gerando sérias conseqüências para o firmatário descuidado. Portanto, quando da normatização da matéria dos documentos eletrônicos, responsabilidades (em relação à segurança de uso e à custódia do meio técnico capaz de produzir a firma eletrônica) deverão ser criteriosamente estabelecidas, como forma de conscientizar os usuários em relação à importância do cuidado em relação ao aspecto segurança. .

A situação do Brasil, em termos de estudos tendentes a um melhor conhecimento e sistematização da matéria, não é animadora. Pouco se aborda o fenômeno maior, que é a "Sociedade da Informação", e, menos ainda, se fala de uma de suas conseqüências, que são os documentos eletrônicos. Em termos de iniciativa legislativa, existe um projeto de lei, que foi discutido com alguns setores da sociedade, OAB, de São Paulo por exemplo, mas ainda não foi colocado para discussão em plenário na Câmara dos Deputados. Em termos práticos, já há empresas operando com uso da criptografia assimétrica e certificação das assinaturas. O que se verifica são meras tentativas de uso operacional dos documentos eletrônicos, com algumas preocupações com aspectos jurídicos. Para outros tudo funciona baseado na confiança mútua, o que acaba por gerar situações de potencial risco jurídico.

Quanto à possibilidade de utilização dos documentos eletrônicos à luz do ordenamento vigente, sem edição de normatização complementar adequada, pensa-se que tal alternativa se mostra temerária. Documentos eletrônicos assim utilizados (os quais poderiam ser chamados de "hermenêuticos"), sujeitar-se-iam a ter uma vida claudicante. Observe-se que a tarefa de estabelecimento de um modelo prático a ser utilizado ficaria a cargo de cada pessoa, conforme seus critérios e conhecimentos subjetivos acerca do tema. Isso poderia gerar documentos eletrônicos com eficácia probatória diminuída, por deficiência em sua formação. Além disso, a interpretação necessária, das normas existentes, sempre algo muito subjetivo, daria margem a soluções diversas para idênticas situações. Vê-se, pois, que a subjetividade envolvida seria tão onipresente que acabaria por gerar grande

insegurança jurídica, correndo-se o risco de fazer o uso dos documentos eletrônicos cair em descrédito.

Um dos principais papéis das novas normas legais necessárias seria, justamente, padronizar e regular os aspectos necessários e essenciais, a fim de que os operadores jurídicos e a própria sociedade, possam saber, exatamente, como formar um documento eletrônico portador de plena eficácia probatória. Para finalizar, é preciso enfatizar a necessidade de maiores estudos e debates acerca do tema da presente pesquisa, que se apresenta vasto e possuidor de muitos meandros e peculiaridades. A troca de idéias é fundamental para a conformação de uma base para sistematização. Somente assim é que se poderá formar um conhecimento sólido e adequado, capaz de possibilitar a produção de normas que abrirão espaço para a popularização do uso dos documentos eletrônicos com validade jurídica.

A par de tais estudos, é de vital importância uma abordagem da questão cultural envolvida, procurando-se a superação do uso da informática, apenas, como mera ferramenta para acelerar a geração de papel. É evidente que o documento tradicional já não condiz com a agilidade exigida pela sociedade atual e, portanto, está claro que haverá uma mudança. Só resta saber quando e de que forma ela se dará. Não há dúvida que, em virtude das inúmeras vantagens que o documento eletrônico pode apresentar em relação às formas de documentação tradicional – dentre as quais as economias de tempo e espaço, a transmissibilidade, a duplicabilidade e o baixo custo –, a difusão de seu uso cotidiano, mais do que uma mera concessão ao conforto ou a uma efêmera modernidade, será um caso de imperativa necessidade.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRE, Sílvio. O ciberespaço e o direito. Disponível em: **<http://www.iaccess.com.br/berjur/.html>.** Acessado em 24 de maio de 2003.

ARRUDA JÚNIOR, Itamar. Considerações ao PL m. 1589/99. Disponível em: **http://www.e-juridico.com.br.** Acessado em 20 de setembro de 2003.

AUGUSTO, Alexandre. **Os novos documentos eletrônicos.** São Paulo, n. 5, p. 35-50,maio 1993.

BANGEMANN, Martin et al. Europe and the global information society: recommendations to the European Council. Disponível em: **<http://www.echo./eudoc/eport.html>.** Acessado em 02 de junho de 2003.

BRASIL. Angela Bittencourt. O documento físico e o documento eletrônico. Disponível em: **http://www.datavenia.com/proj.htm**. Acessado em 03 de maio de 2003.

BRASIL. Ministério das Relações Exteriores: Departamento de Cooperação Científica, Técnica e Recnológica. Lei modelo da UNCITRAL sobre comércio eletrônico com guia para sua incorporação ao direito interno. Disponível em: **http://www.doct.mre.gov.br/seminario_lei.htm.** Acessado em 03 de maio de 2003.

BRASÍLIA. Medida Provisória: 2.200-2. Institui a Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil. Disponível em**: http://wwwt.senado.gov.br/**

BRASÍLIA. Projeto Decreto-Lei 1.589/1999. Dispõe Sobre a Validade Jurídica e o Valor Probante do Documento Eletrônico. Disponível em: **http://www.camara.gov.br/.**

BUONOMO, Giovanni. Atti e documenti in forma digitale. Disponível em: **<http://www.interlex.com/digit/buono.htm>.** Acessado em 16 de agosto de 2003.

CAMMARATA, Manlio. Il documento elettronico: "key escrow", una questione molto delicata. Disponível em: **<http://www.interlex.com/digit/mc.htm>.** Acessado em 24 de maio de 2003.

CASTRO, Aldemario Araujo. O documento eletrônico e a assinatura digital: uma visão geral. Disponível em: **<http://www.direitonaweb.adv.br/doutrina/dinfo/Aldemario_A_Castro_(DINFO_0003).htm>**. Acessado em 03 de abril de 2003.

_____, Aldemario Araujo. Validade jurídica de documentos eletrônicos. Considerações jurídicas sobre o projeto de Lei apresentado pelo governo Federal. Disponível em: **http://www.e-juridico.com.br.** Acessado em 20 de setembro de 2003.

CHIOVENDA, Giuseppe. **Instituições de direito Processual Civil.** Campinas: Bookseller, 1998.

FROOMKIN, A. Michael. The essential role of thrusted third parties in electronic commerce. Version. Disponível em: **<http://www.miami.edu/articles/trusted.htm>**. Acessado em 14 de agosto de 2003.

GANDINI, J. A. D.; SALOMÃO, D. P. da S; JACOB, C. A validade jurídica dos documentos digitais. Disponível em: **http://www1.jus.com.br/doutrina/texto.asp?id=3165.** Acessado em 25 de maio de 2003.

GICO JÚNIOR, Ivo Teixeira. O documento eletrônico como meio de prova no Brasil. Disponível em **http://www.alfa.rede.org/uplaad/revista**. Acessado em 29 de junho de 2003.

GIUSTOZZI, Corrado. La crittografia a chiave pubblica e l'algoritmo RSA: terminologia crittografica. Disponível em: **<http://www.interlex.com/digit/rado.htm>.** Acessado em 02 de junho de 2003.

GOIS, JÚNIOR, José Caldas. **O direito na era das redes**: a liberdade e o delito no ciberespaço. São Paulo: Edipro, 2001.

KALINSKI JÚNIOR, E.; BURTON S.. Autenticação de documentos digitais por sistemas criptográficos de chave pública. Disponível em: **<http://www.interlex.com/docdigit/.htm>**. Acessado em 24 de maio de 2003.

LIMA NETO, José Henrique Barbosa Moreira. Aspectos jurídicos do documento eletrônico. Disponível em: **<http://www.jus.com.br/doutrina.html**. Acessado em 14 de agosto de 2003.

MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. Disponível em: **<http://members.com/marcacini/celet.pdf>.** Acessado em 02 de junho de 2003.

MERCADO, Luís Paulo Leopoldo. Novas tecnologias na educação: reflexões sobre a prática. Maceió: EDUFAL, 2002.

MICCOLI, Mario. Cybernotary, Consiglio Nazionale del Notariato – Forum di Informatica Giuridica. Disponível em: **<http://www.notariato/forum/bernot.zip.** Acessado em 02 de junho de 2003.

MONTI, Andrea. *Il documento informatico nei rapporti di diritto privato.* Disponível em: **<http://www.interlex.com/docdigit/.htm>**. Acessado em 24 de maio de 2003.

OLIVEIRA, Juarez de. **Código Tributário Nacional:** Lei 5.172 de 25 outubro de 1966. São Paulo: Saraiva, 1994.

ROGNETTA, Giorgio. *Diritto virtuale e crittografia asimmetrica*. Disponível em: **<http://www.cibernet.it/jura/jura/pp/rognetta/zaleuco2.htm>.** Acessado em 02 de junho de 2003.

SAKAMOTO, Marcos. O Direito das Gentes e a Informática. Revista Teia Jurídica. Disponível em: **<http://teiajuridica.com.** Acessado em 28 de junho de 2003.

SANTOS, Moacyr Amaral. **Primeiras linhas de direito Processual Civil**. São Paulo: Saravia, 1972.

TAGLINO, Daniela. Il valore giuridico del documento elettronico. Disponível em: **<http://freepage.logicom/Page/i.zip>.** Acessado em 28 de julho de 2003.

VOLPI, Marlon Marcelo. Assinatura Digital: aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books, 2001.

XEXÉO, Geraldo. Autenticação de documentos digitais por sistemas criptográficos de chave pública. Disponível em: **http://www.cos.ufrj.br//talk/assina.htm.** Acessado em 28 de julho de 2003.

ZAGAMI, Raimondo. Firme "digitali", crittografia e validità del documento elettronico. Il Diritto dell'Informazione e dell'Informatica. Disponível em: **<http://www.notariato/forum/gami.zip>.** Acessado em 02 de junho de 2003.

6. ANEXOS

ANEXO I - SUBTITUTIVO AO PROJETO DE LEI 1.489/99 E 1.589/99-
RELATOR DEPUTADO JULIO SEMEGHINI

E-commerce/ Íntegra do substitutivo

Substitutivo da Comissão Especial destinada a apreciar e proferir parecer ao Projeto de Lei 1483/99, do deputado Dr. Hélio (PDT-SP), que institui a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico.

Dispõe sobre a validade jurídica e o valor probante do documento eletrônico e da assinatura digital, regula a certificação digital, institui normas para as transações de comércio eletrônico e dá outras providências. O Congresso Nacional decreta:

TÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta lei dispõe sobre a validade jurídica e o valor probante do documento eletrônico e da assinatura digital, regula a certificação digital, institui normas para as transações de comércio eletrônico e estabelece sanções administrativas e penais aplicáveis.

Art. 2º Para os efeitos desta lei, considera-se: I - documento eletrônico: a informação gerada, enviada, recebida, armazenada ou comunicada por meios eletrônicos, ópticos, opto-eletrônicos ou similares; II - assinatura digital: resultado de um processamento eletrônico de dados, baseado em sistema criptográfico assimétrico, que permite comprovar a autoria e integridade de um documento eletrônico cifrado pelo autor com o uso da chave privada; III - criptografia assimétrica: modalidade de cifragem que utiliza um par de chaves distintas e interdependentes, denominadas chaves pública e privada, de modo que a mensagem codificada por uma das chaves só possa ser decodificada com o uso da outra chave do mesmo par; IV - entidade certificadora: pessoa jurídica que esteja apta a expedir certificado digital e oferecer ou facilitar serviços de registro e datação da transmissão e da recepção de documentos eletrônicos; V - certificado digital: documento eletrônico expedido por entidade certificadora que atesta a titularidade de uma chave pública; VI - autoridade credenciadora: órgão responsável pelo credenciamento voluntário de entidades certificadoras.

Parágrafo único. O Poder Público determinará a aplicação das disposições constantes desta lei para a assinatura digital a outros processos que satisfaçam os requisitos operacionais e de segurança daquela.

TÍTULO II

DO DOCUMENTO ELETRÔNICO E DA ASSINATURA DIGITAL

Capítulo I - Dos efeitos jurídicos do documento eletrônico e da assinatura digital

Art. 3º Não serão negados efeitos jurídicos, validade e eficácia ao documento eletrônico, pelo simples fato de apresentar-se em forma eletrônica.

§ 1º Considera-se original o documento eletrônico digitalmente assinado por seu autor.

§ 2º Considera-se cópia o documento eletrônico resultante da digitalização de documento físico, bem como a materialização de documento eletrônico original em forma impressa, microfilmada ou registrada em outra mídia que permita a sua leitura em caráter permanente.

Art. 4º As declarações constantes de documento eletrônico original presumem-se verdadeiras em relação ao signatário, desde que a assinatura digital: I - seja única e exclusiva para o documento assinado; II - seja passível de verificação pública; III - seja gerada com chave privada pertencente ao signatário e mantida sob o seu exclusivo controle; IV - esteja ligada ao documento eletrônico de tal modo que se o conteúdo deste se alterar, a assinatura digital estará invalidada; V - não tenha sido gerada posteriormente à expiração, revogação ou suspensão das chaves.

Art. 5º A titularidade da chave pública poderá ser provada por todos os meios de direito, vedada a prova exclusivamente testemunhal. Parágrafo único. Não será negado valor probante ao documento eletrônico e sua assinatura digital, pelo simples fato de esta não se basear em chaves certificadas por uma entidade certificadora credenciada.

Art. 6º Presume-se verdadeira, entre os signatários, a data do documento eletrônico, sendo lícito, porém, a qualquer deles, provar o contrário por todos os meios de direito.

§ 1º Após expirada ou revogada a chave de algum dos signatários, compete à parte a quem o documento beneficiar a prova de que a assinatura foi gerada anteriormente à expiração ou revogação.

§ 2º Entre os signatários, para os fins do parágrafo anterior, ou em relação a terceiros, considerar-se-á datado o documento particular na data: I - em que foi registrado; II - da sua apresentação em repartição pública ou em juízo; III - do ato ou fato que estabeleça, de modo certo, a anterioridade da formação do documento e respectivas assinaturas.

Art. 7º Aplicam-se ao documento eletrônico as demais disposições legais relativas à prova documental que não colidam com as normas deste Título. Capítulo II - Da falsidade dos documentos eletrônicos.

Art. 8º O juiz apreciará livremente a fé que deva merecer o documento eletrônico, quando demonstrado ser possível alterá-lo sem invalidar a assinatura, gerar uma assinatura eletrônica idêntica à do titular da chave privada, derivar a chave privada a partir da chave pública, ou pairar razoável dúvida sobre a segurança do sistema criptográfico utilizado para gerar a assinatura.

Art. 9º Havendo impugnação do documento eletrônico, incumbe o ônus da prova: I - à parte que produziu o documento, quanto à autenticidade da chave pública e quanto à segurança do sistema criptográfico utilizado; II - à parte contrária à que produziu o documento, quando alegar apropriação e uso da chave privada por terceiro, ou revogação ou suspensão das chaves.

TÍTULO III

DOS CERTIFICADOS DIGITAIS

Capítulo I - Dos certificados digitais e seus efeitos

Art. 10 Os certificados digitais produzirão, entre o ente certificante e a pessoa certificada, os efeitos jurídicos definidos no contrato por eles firmado. Parágrafo único. Em relação a terceiros, a certificação produz os efeitos que o ente certificante declarar à praça, se mais benéficos a aqueles.

Art. 11 Para fazer prova em relação ao titular indicado no certificado, é necessário que, no ato de sua expedição: I - o requerente seja pessoalmente identificado pela entidade certificadora; II - o requerente reconheça ser o titular da chave privada, identificada com elementos suficientes para sua individualização; III - sejam arquivados registros físicos comprobatórios dos fatos previstos nos incisos anteriores, assinados pelo requerente, a serem exibidos em juízo, quando necessário.

Art. 12 Os certificados digitais deverão conter pelo menos as seguintes informações: I - identificação e assinatura digital da entidade certificadora; II - identificação da chave pública a que o certificado se refere e do seu titular, caso o certificado não seja diretamente apensado àquela; III - data de emissão e prazo de validade; IV - nome do titular e poder de representação de quem solicitou a certificação, no caso do titular ser pessoa jurídica; V - data de nascimento do titular, se pessoa física; VI - elementos que permitam identificar o sistema de criptografia utilizado.

§ 1º Na falta de informação sobre o prazo de validade do certificado, este será de dois anos, contados da data de emissão. § 2º A regulamentação desta lei poderá determinar a inclusão de informações adicionais no certificado digital, em respeito a requisitos específicos conforme a finalidade do certificado.

Art. 13 São obrigações do titular do certificado digital: I - fornecer as informações solicitadas pela entidade certificadora, observado o inciso VII do art. 18; II - manter sigilo e controle da chave privada; III - solicitar a revogação dos certificados nos casos de quebra de confidencialidade ou comprometimento da segurança de sua chave privada.

§ 1º O titular do certificado digital será civilmente responsável pela falsidade das informações fornecidas à entidade certificadora, sem prejuízo das sanções penais aplicáveis, bem como pelo descumprimento das obrigações previstas no caput deste artigo.

§ 2º Exclui-se a responsabilidade do titular do certificado, decorrente do inciso II do caput deste artigo, quando o uso da assinatura digital lhe for imposto ou os meios a ele fornecidos para a criação das chaves não ofereçam garantias de auditabilidade e controle do risco.

Capítulo II - Da suspensão e revogação de certificados digitais.

Art. 14 A entidade certificadora suspenderá temporariamente o certificado digital: I - a pedido por escrito do titular, devidamente identificado para o evento, ou de seu representante legal; II - quando existam fundadas razões para crer que: a. o certificado foi emitido com base em informações errôneas ou falsas; b. as informações nele contidas deixaram de ser condizentes com a realidade; ou c. a confidencialidade da chave privada foi violada.

Parágrafo único. A suspensão do certificado digital com fundamento no inciso II deste artigo será sempre motivada e comunicada prontamente ao titular, bem como imediatamente inscrita no registro do certificado.

Art. 15 A entidade certificadora deverá revogar um certificado digital: I - a pedido por escrito do titular, devidamente identificado para o evento, ou de seu representante legal; II - quando expirado seu prazo de validade; III - de ofício ou por determinação do Poder Judiciário, caso se verifique que o certificado foi expedido com base em informações falsas; IV - de ofício, se comprovadas as razões que fundamentaram a suspensão prevista no inciso II do art. 14; V - tratando-se de entidade certificadora credenciada, por determinação da autoridade credenciadora, na forma do inciso IX do art. 24 desta lei; VI - se a entidade certificadora vier a encerrar suas atividades sem que seja sucedida por outra entidade nos termos do § 1º do art. 20 desta lei; VII - por falecimento ou interdição do signatário, se pessoa física, ou no caso de falência ou dissolução de sociedade, se pessoa jurídica.

TÍTULO IV

DAS ENTIDADES CERTIFICADORAS

Capítulo I - Dos princípios gerais

Art. 16 A atividade de certificação digital será regida pelos seguintes princípios: I - liberdade de contratação, observadas as normas de defesa do consumidor; II - preservação da privacidade do usuário; III - dispensa de autorização prévia; IV - direito do usuário a ser adequadamente informado sobre o funcionamento dos sistemas criptográficos utilizados e os procedimentos técnicos necessários para armazenar e utilizar com segurança a chave privada; V - vedação ao depósito de chaves privadas pela entidade certificadora.

Art. 17 Poderão ser entidades certificadoras as pessoas jurídicas de direito público ou privado, constituídas sob as leis brasileiras e com sede e foro no País. Parágrafo único. O funcionamento de entidade certificadora independe do credenciamento previsto no art. 21 desta lei, sendo obrigatória apenas a comunicação, ao Poder Público, do início das atividades.

Capítulo II - Dos deveres e responsabilidades das entidades certificadoras

Art. 18 As entidades certificadoras deverão: I - emitir certificados conforme o solicitado ou acordado com o signatário da assinatura digital; II - implementar sistemas de segurança adequados à criação, emissão e arquivamento de certificados digitais; III - implementar sistemas de proteção adequados para impedir o uso indevido da informação fornecida pelo requerente de certificado digital; IV - operar sistema de suspensão e revogação de certificados, procedendo à imediata publicação nas hipóteses previstas nesta lei; V - tornar disponível, em tempo real e mediante acesso eletrônico remoto, lista de certificados emitidos, suspensos e revogados; VI - manter quadro técnico qualificado; VII - solicitar do requerente de certificado digital somente as informações necessárias para sua identificação e emissão do certificado; VIII - manter confidencialidade sobre todas as informações obtidas do titular que não constem do certificado; IX - exercer as atividades de emissão, suspensão e revogação de certificados dentro dos limites do território brasileiro.

§ 1º Os dados pessoais não serão usados para outra finalidade que não a de certificação, salvo se consentido expressamente pelo requerente, por cláusula em destaque, que não esteja vinculada à realização da certificação. § 2º A quebra da confidencialidade das informações de que trata o inciso VIII do caput deste artigo, quando determinada pelo Poder Judiciário, respeitará os mesmos procedimentos previstos em lei para a quebra do sigilo bancário.

Art. 19 A entidade certificadora é responsável civilmente pelos danos sofridos pelo titular do certificado e por terceiros, decorrentes da falsidade dos certificados por ela emitidos ou do descumprimento das obrigações previstas no art. 18.

Art. 20 O registro de certificado expedido por uma entidade certificadora deve ser por ela conservado até o término do prazo exigido pela lei que regular o negócio jurídico associado ao certificado, não inferior, em qualquer caso, a vinte anos.

§ 1º No caso de pretender cessar voluntariamente a sua atividade ou tiver a falência decretada por sentença transitado em julgado, a entidade certificadora deverá: I - comunicar a intenção à autoridade credenciadora com antecipação mínima de três meses; II - comunicar aos titulares dos certificados por ela emitidos, com antecedência de trinta dias, a revogação dos certificados ou a sua transferência a outra entidade certificadora.

§ 2º No caso de revogação dos certificados mencionados no inciso II do § 1º, emitidos por entidade certificadora credenciada, a guarda da respectiva documentação será de responsabilidade da autoridade credenciadora.

Capítulo III - Do credenciamento voluntário

Art. 21 Poderão ser credenciadas pela autoridade competente, mediante requerimento, as entidades certificadoras que preencham os seguintes requisitos, conforme a regulamentação desta lei: I - capacitação técnica para prestar os serviços de certificação, nos termos definidos nesta lei; II - recursos de segurança

física e lógica compatíveis com a atividade de certificação; III - capacidade patrimonial adequada à atividade de certificação, ou manutenção de contrato de seguro suficiente para cobertura dos danos eventualmente causados; IV - integridade e independência no exercício da atividade de certificação; V - garantia da qualidade das informações transmitidas aos requerentes, quanto ao uso e procedimentos de segurança dos sistemas utilizados.

Art. 22 Às entidades certificadoras credenciadas será atribuído um sinal gráfico, atestando que atendem aos requisitos previstos no art. 21.

Parágrafo único. O credenciamento permitirá à entidade certificadora utilizar, com exclusividade, o sinal previsto no caput deste artigo, bem como a designação de "entidade certificadora credenciada".

Art. 23 O credenciamento será revogado, sem prejuízo de outras sanções aplicáveis na forma desta lei, nos casos em que: I - for obtido por meio de declaração falsa ou expediente ilícito; II - deixar de se verificar algum dos requisitos previstos no art. 21; III - deixar a entidade certificadora de exercer suas atividades por período superior a doze meses; IV - ocorrerem irregularidades insanáveis na administração, organização ou no exercício das atividades da entidade certificadora; V - forem praticados atos ilícitos ou que coloquem em perigo a confiança do público na certificação.

§ 1º A revogação compete à autoridade credenciadora, em decisão fundamentada, devendo a entidade certificadora ser notificada no prazo de sete dias úteis.

§ 2º A autoridade credenciadora dará ampla publicidade à decisão. Capítulo IV - Da autoridade credenciadora

Art. 24 O Poder Público designará autoridade credenciadora, a quem caberá: I - apreciar pedido de credenciamento apresentado por entidade certificadora; II - solicitar emendas ao pedido ou informações complementares e proceder, diretamente ou por terceiros, às averiguações e inspeções necessárias à apreciação do pedido; III - estabelecer condições adicionais desde que necessárias para assegurar o cumprimento das disposições legais e regulamentares aplicáveis ao exercício da atividade de certificação; IV - expedir declaração de credenciamento, estabelecendo o seu prazo de validade; V - conduzir auditorias periódicas para verificar se as condições do credenciamento se preservam, na forma da regulamentação; VI - manter e divulgar relação de entidades certificadoras credenciadas; VII - divulgar amplamente a suspensão ou revogação de credenciamento; VIII - aplicar sanções administrativas nas hipóteses previstas nesta lei; IX - determinar a suspensão temporária ou a revogação de certificado digital emitido por entidade certificadora por ela credenciada quando constatada irregularidade.

TÍTULO V

DO COMÉRCIO ELETRÔNICO

Capítulo I - Da contratação no âmbito do comércio eletrônico

Art. 25 A oferta de bens, serviços e informações não está sujeita a qualquer tipo de autorização prévia pelo simples fato de ser realizada por meio eletrônico. Art. 26 Sem prejuízo das disposições do Código Civil, a manifestação de vontade das partes contratantes, nos contratos celebrados por meio eletrônico, dar-se-á no momento em que: I - o destinatário da oferta enviar documento eletrônico manifestando, de forma inequívoca, a sua aceitação das condições ofertadas; e II - o ofertante transmitir resposta eletrônica transcrevendo as informações enviadas pelo destinatário e confirmando seu recebimento.

§ 1º A proposta de contrato por meio eletrônico obriga o proponente quando enviada por ele próprio ou por sistema de informação por ele programado para operar automaticamente.

§ 2º A manifestação de vontade a que se refere o caput deste artigo será processada mediante troca de documentos eletrônicos, observado o disposto nos arts. 27 a 29 desta lei.

Art. 27 O documento eletrônico considera-se enviado pelo remetente e recebido pelo destinatário se for transmitido para o endereço eletrônico definido por acordo das partes e neste for recebido.

Art. 28 A expedição do documento eletrônico equivale: I - à remessa por via postal registrada, se assinado de acordo com os requisitos desta lei, por meio que assegure sua efetiva recepção; e II - à remessa por via postal registrada e com aviso de recebimento, se a recepção for comprovada por mensagem de confirmação dirigida ao remetente e por este recebida.

Art. 29 Para os fins do comércio eletrônico, a fatura, a duplicata e demais documentos comerciais, quando emitidos eletronicamente, obedecerão ao disposto na legislação comercial vigente. Capítulo II - Da proteção e defesa do consumidor no âmbito do comércio eletrônico.

Art. 30 Aplicam-se ao comércio eletrônico as normas de defesa e proteção do consumidor vigentes no País, naquilo que não conflitar com esta Lei. Art. 31 A oferta de bens, serviços ou informações por meio eletrônico deve ser realizada em ambiente seguro, devidamente certificado, e deve conter claras e inequívocas informações sobre: I - nome ou razão social do ofertante; II - número de inscrição do ofertante no respectivo cadastro geral do Ministério da Fazenda e, em se tratando de serviço sujeito a regime de profissão regulamentada, o número de inscrição no órgão fiscalizador ou regulamentador; III - domicílio ou sede do ofertante; IV - identificação e sede do provedor de serviços de armazenamento de dados; V - número de telefone e endereço eletrônico para contato com o ofertante; VI - tratamento e armazenamento, pelo ofertante, do contrato ou das informações fornecidas pelo destinatário da oferta; VII - instruções para arquivamento do contrato eletrônico pelo aceitante, bem como para sua recuperação em caso de necessidade; e VIII - sistemas de segurança empregados na operação.

Art. 32 Para o cumprimento dos procedimentos e prazos previstos na legislação de proteção e defesa do consumidor, os adquirentes de bens, serviços e informações por meio eletrônico poderão se utilizar da mesma via de comunicação adotada na contratação para efetivar notificações e intimações extra-judiciais.

§ 1º Para os fins do disposto no caput deste artigo, os ofertantes deverão, no próprio espaço que serviu para o oferecimento de bens, serviços e informações, colocar à disposição dos consumidores área específica, de fácil identificação, que permita o armazenamento das notificações ou intimações, com a respectiva data de envio, para eventual comprovação.

§ 2º O ofertante deverá transmitir uma resposta automática aos pedidos, mensagens, notificações e intimações que lhe forem enviados eletronicamente, comprovando o recebimento.

Capítulo III - Da solicitação e uso das informações privadas

Art. 33 O ofertante somente poderá solicitar do consumidor informações de caráter privado necessárias à efetivação do negócio oferecido, devendo mantê-las em sigilo, salvo se prévia e expressamente autorizado pelo respectivo titular a divulgá-las ou cedê-las.

§ 1º A autorização de que trata o caput deste artigo constará em destaque, não podendo estar vinculada à aceitação do negócio.

§ 2º Sem prejuízo de sanção penal, responde por perdas e danos o ofertante que solicitar, divulgar ou ceder informações em violação ao disposto neste artigo. Capítulo IV - Das obrigações e responsabilidades dos provedores

Art. 34 Os provedores de acesso que assegurem a troca de documentos eletrônicos não podem tomar conhecimento de seu conteúdo, nem duplicá-los por qualquer meio ou ceder a terceiros qualquer informação, ainda que resumida ou por extrato, sobre a existência ou sobre o conteúdo desses documentos, salvo por indicação expressa do seu remetente.

§ 1º Igual sigilo recai sobre as informações que não se destinem ao conhecimento público armazenadas no provedor de serviços de armazenamento de dados.

§ 2º Somente mediante ordem do Poder Judiciário poderá o provedor dar acesso às informações acima referidas, sendo que as mesmas deverão ser mantidas, pelo respectivo juízo, em segredo de justiça.

Art. 35 O provedor que forneça serviços de conexão ou de transmissão de informações, ao ofertante ou ao adquirente, não será responsável pelo conteúdo das informações transmitidas.

Art. 36 O provedor que forneça ao ofertante serviço de armazenamento de arquivos e sistemas necessários para operacionalizar a oferta eletrônica de bens, serviços ou informações não será responsável pelo seu conteúdo, salvo, em ação regressiva do ofertante, se:

I - deixou de atualizar as informações objeto da oferta, tendo o ofertante tomado as medidas adequadas para efetivar as atualizações, conforme instruções do próprio provedor; ou II - deixou de arquivar as informações ou, tendo-as arquivado, foram elas destruídas ou modificadas, tendo o ofertante tomado as medidas adequadas para seu arquivamento, segundo parâmetros estabelecidos pelo provedor.

Art. 37 O provedor que forneça serviços de conexão ou de transmissão de informações, ao ofertante ou ao adquirente, não será obrigado a vigiar ou fiscalizar o conteúdo das informações transmitidas.

Art. 38 Responde civilmente por perdas e danos, e penalmente por co-autoria do delito praticado, o provedor de serviço de armazenamento de arquivos que, tendo conhecimento inequívoco de que a oferta de bens, serviços ou informações constitui crime ou contravenção penal, deixar de promover sua imediata suspensão ou interrupção de acesso por destinatários, competindo-lhe notificar, eletronicamente ou não, o ofertante, da medida adotada.

TÍTULO VI

DAS SANÇÕES ADMINISTRATIVAS

Art. 39 As infrações às normas estabelecidas nos Títulos II, III e IV desta lei, independente das sanções de natureza penal e reparação de danos que causarem, sujeitam a entidade infratora à penalidade de multa de dez mil reais a um milhão de reais cominada, no caso de entidade credenciada, à suspensão de credenciamento ou à sua revogação.

§ 1º As sanções estabelecidas neste artigo serão aplicadas pela autoridade credenciadora, considerando-se a gravidade da infração, vantagem auferida, capacidade econômica, e eventual reincidência.

§ 2º A pena de suspensão poderá ser imposta por medida cautelar antecedente ou incidente de procedimento administrativo.

Título VII

Das SANÇÕES PENAIS

Art. 40 A quebra de sigilo das informações de que trata o inciso VIIII do art. 18 e os arts. 33 e 34 desta lei constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos.

Art. 41 Equipara-se ao crime de falsificação de papéis públicos, sujeitando-se às penas do art. 293 do Código Penal, a falsificação, com fabricação ou alteração, de certificado digital de ente público.

Parágrafo único. Incorre na mesma pena de crime de falsificação de papéis públicos quem utilizar certificado digital público falsificado.

Art. 42 Equipara-se ao crime de falsificação de documento público, sujeitando-se às penas previstas no art. 297 do Código Penal, a falsificação, no todo ou em parte, de documento eletrônico público, ou a alteração de documento eletrônico público verdadeiro.

Parágrafo único. Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aplica-se o disposto no § 1º do art. 297 do Código Penal.

Art. 43 Equipara-se ao crime de falsidade de documento particular, sujeitando-se às penas do art. 298 do Código Penal, a falsificação, no todo ou em parte, de

certificado ou documento eletrônico particular, ou alteração de certificado ou documento eletrônico particular verdadeiro.

Art. 44 Equipara-se ao crime de falsidade ideológica, sujeitando-se às penas do art. 299 do Código Penal, a omissão, em documento ou certificado eletrônico público ou particular, de declaração que dele devia constar, ou a inserção ou fazer com que se efetue inserção, de declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante.

Parágrafo único. Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aplica-se o disposto no parágrafo único do art. 299 do Código Penal.

Art. 45 Equipara-se ao crime de supressão de documento, sujeitando-se às penas do art. 305 do Código Penal, a destruição, supressão ou ocultação, em benefício próprio ou de outrem, de documento eletrônico público ou particular verdadeiro, de que não se poderia dispor.

Art. 46 Equipara-se ao crime de extravio, sonegação ou inutilização de documento, sujeitando-se às penas previstas no art. 314 do Código Penal, o extravio de qualquer documento eletrônico, de que se tem a guarda em razão do cargo, ou sua sonegação ou inutilização, total ou parcial.

Título VIII

DAS DISPOSIÇÕES GERAIS

Art. 47 As certificações estrangeiras de assinaturas digitais terão o mesmo valor jurídico das expedidas no País, desde que a entidade certificadora esteja sediada e seja devidamente reconhecida em país signatário de acordos internacionais relativos ao reconhecimento jurídico daqueles certificados, dos quais seja parte o Brasil.

Art. 48 Para a solução de litígios de matérias objeto desta lei poderá ser empregado sistema de arbitragem, obedecidos os parâmetros da Lei n° 9.037, de 23 de setembro de 1996, dispensada a obrigação decretada no § 2° de seu art. 4°, devendo, entretanto, efetivar-se destacadamente a contratação eletrônica da cláusula compromissória.

Título IX

DISPOSIÇÕES FINAIS

Art. 49 O Poder Executivo regulamentará a presente lei no prazo de noventa dias. Art. 50 Esta lei entra em vigor em cento e vinte dias, contados da data de sua publicação. Sala da Comissão, em 8 de agosto de 2001. Deputado JULIO SEMEGHINI Relator

ANEXO II - MEDIDA PROVISÓRIA 2.200-2 DE 24 DE AGOSTO DE 2001

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA , no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-

Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei nº 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

Fernando Henrique Cardoso
José Gregori
Martus Tavares
Ronaldo Mota Sardenberg